Avaya Video Telephony Solution Release 5.2 Networking Guide

04-603308
Issue 1
May 2009

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 may be incorporated in future releases.

For full legal page information, please see the complete document, Avaya Legal Page for Software Documentation, Document number 03-600758.

To locate this document on the website, simply go to http://www.avaya.com/support **and search for the document number in the search box.**

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 of 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 following Web site:

http://www.avaya.com/support

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.

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 Web site:

http://www.avaya.com/support

Contents

Chapter 1: Introduction 7
Overview of Avaya Video Telephony Solution 7
What's New in this Release 8
Requirements 8
Further Information 8
Managing Video on Your Network 9
Classifying Video Users 9
Set Up Your Bandwidth Pools 10
Sample Scenarios 10

Chapter 2: Design and Deployment Checklist 17
Overview 17
Network and PBX-Network Requirements 18
Feature Interactions and Limitations 20
Avaya Communication Manager Global Administration 22
Avaya Communication Manager Administration for Ad-hoc Video Conferencing 28
Avaya Communication Manager Administration for Polycom Multipoint Stations (VSX and HDX) 29
Avaya Communication Manager Administration for Polycom MGC Systems . . . 30
Avaya Communication Manager Administration for Polycom RMX Systems . . . 33
Polycom MGC Configuration 34
Polycom RMX Configuration 36
Polycom HDX/VSX System Configuration 38
Avaya one-X Communicator 39
Avaya one-X Communicator Performance Issues 40
Priority Bandwidth Management 41
SIP Administration (Global) 42
SIP Trunk Administration 44
SIP Station Administration (OPTIM) 45
SIP Limitations 46

Chapter 3: Setting Up Video Endpoints 49
Required Administration 50
Configure IP Codec Sets 50
Configure IP Network Regions 52
Configure a Station Endpoint for Avaya IP Softphone Release 6.0 and Video Integrator54
Checklist 54

Configuration Procedures 54
Configure a Station Endpoint for Avaya one-X™ Communicator with H.323 . . . 58
Checklist 58
Configuration Procedures 58
Configure Polycom VSX/HDX Series Video Conferencing Systems and V500/V700 Video Calling Systems 62
Checklist 62
Configuration Procedures 62
Configure a Polycom RMX Series Video Conferencing Bridge Platform 72
Checklist 72
Configuration Procedures 72
Configure Ad-hoc Video Conferencing for a Polycom RMX Series Video Conferencing Bridge Platform 81
Checklist 81
Configuration Procedures 81
Display Capacity for Ad-hoc Video Conferencing 95
View Video Conferencing Bridges 95
Configure a Polycom MGC-25 Video Conferencing Bridge Platform for an Avaya S8300 Server 96
Checklist 96
Configuration Procedures 96
Configure Polycom MGC Video Conferencing Bridge Platforms with Avaya S8500 and S87xx Server 100
Trunk Groups 100
Signaling Groups 101
Group Member Assignments 102
Outgoing Rules 103
MGC Limitations 103
Examples 104
Configure Ad-hoc Video Conferencing for a Polycom MGC Video Conferencing Bridge Platform 107
Limitations 107
Checklist 107
Configuration Procedures 108
Display Capacity for Ad-hoc Video Conferencing 114
View Video Conferencing Bridges 114
Configure an Avaya Meeting Exchange 5.1 S6800 Bridge 115
Checklist 115
Things to Keep in Mind 115
Configuration Procedures 116

Configure a Polycom MGC Video Conferencing Bridge Platform as an H.320 Gateway 145
Thing to Keep in Mind 145
Trunk Groups 146
Route Pattern 147
AAR Tables 147
MGC Administration 147
Configure a SE200 Gatekeeper 149
Checklist 149
Configuration Procedures 149
SE200 Limitations 151
Configure a Tandberg Centric 1700 MXP 152
Configure H.323 Stations to Support a Tandberg Centric 1700 MXP 152
Configure a Tandberg Centric 1700 MXP 154
Configure a Tandberg Centric 150 MXP 156
Configure H.323 Stations to Support a Tandberg Centric 150 MXP 157
Configure a Tandberg Centric 150 MXP 158
Tandberg Endpoint Limitations 160
Configure Unauthenticated H.323 Endpoints 161
Enabling Licensing 161
Administering the Station 161
Configuring Third Party Pause 162
Configure a Direct Routing Gatekeeper 166
Thing to Keep in Mind 166
Checklist 166
Configuration Procedures 166
Configure Video Trunks between Two Avaya Communication Manager Systems 171
Checklist 171
Configuration Procedures 171
Monitor the Status of Video Bandwidth Usage 174
Communication Manager Selection of Video Bridge 174
Ad-hoc Licensing Considerations 175

Index 177

Chapter 1: Introduction

Overview of Avaya Video Telephony Solution

The Avaya Video Telephony Solution enables Avaya Communication Manager 5.2 to merge a set of enterprise features with videoconferencing adjuncts.

Note:

Avaya Communication Manager 5.2 is a H.323 to SIP video signaling gateway to support mixed protocol video deployments.

The Avaya Video Telephony Solution unifies voice over IP with video, web applications, Avaya one-X™ Communicator (video-enabled version), third-party gatekeepers, and other H.323 endpoints. With the Avaya Video Telephony Solution, you can provide video for desktop and group communications.

The Avaya Video Telephony Solution supports video calls on the following products:

- Avaya one-X™ Communicator
- IP Softphone Release 6.0 and Video Integrator
- Polycom HDX series video conferencing system
- Polycom VSX series video conferencing system with Release 8.5.3 or later
- Polycom V500/V700 video calling system
- Polycom RMX series video conferencing bridge platform
- Polycom MGC video conferencing bridge platform with Release 8.0.0.27
- Avaya Meeting Exchange 5.1 S6800 bridge
- SE200 gatekeeper
- Tandberg Centric 1700 MXP
- Tandberg Centric 150 MXP
- Unauthenticated H.323 endpoints

Note:

You must perform a network readiness or network assessment to ensure your network is capable of supporting the high bandwidth demands of video over IP. You should also consider implementing QoS across your network. For more information on configuring QoS, see the Avaya Communication Manager documentation, which is available on support.avaya.com. In particular, the guide *Administration for Network Connectivity for Avaya Communication Manager* contains relevant information.

What's New in this Release

Avaya Video Telephony Solutions Release 5.2 introduces the following new features and enhancements:

- Added support for Siren 22 wideband audio codecs when shuffled to direct-IP audio connectivity between the endpoints/MCUs.

  Note:

  A limitation of two Communication Manager servers apply. Tandeming of more PBXs is not supported and remains single-band audio.

- H.245 signaling support for Polycom's Lost Packet Recovery (LPR) feature.
- Improved video interoperability with third party gatekeepers and PBXs including Cisco's Call Manager (limited to basic video calling).
- A one button Instant Transfer from a deskset to a video executive desktop system, for example a HDX4000, to allow the user to make all call originations from the deskset.
- Support for one-X communicator with H.323 video only, including support for VGA resolution. One-X communicator SIP video will be available in a future AVTS release.
- The display of the status of each video bridge on the list video-bridge command.

Requirements

Video Telephony Solution Release 5.2 requires:

- An S8xxx server that is running Avaya Communication Manager 5.2.
- Avaya licensing keys (for RMX and HDX systems)

Further Information

For more information on the Avaya Video Telephony Solution and the Avaya Communication Manager, see support.avaya.com. This Website contains all the customer documentation for this release. Useful documents include:

- Administration for Network Connectivity for Avaya Communication Manager

Managing Video on Your Network

Before configuring video endpoints, you should determine how you want to manage video on your network. To control how your bandwidth is used, you must:

1. Determine whether you want to provide some endpoints with video whenever possible.
2. Set up your bandwidth pools.

Classifying Video Users

You can identify two types of video stations: priority video stations and normal video stations. Priority stations have an increased likelihood of receiving bandwidth and may also be allocated a larger maximum bandwidth per call. By having a larger maximum bandwidth per call, priority video stations may receive better quality and more reliable video during calls. Priority video stations will have an increased likelihood of having video on outgoing calls they make. However, they might not receive video on incoming calls they receive from “non-priority” stations due to the following conditions:

- No bandwidth is available.
- No “normal” bandwidth is available even though priority bandwidth is available. Since the call is made by a normal (non-priority) video station, this station would not have access to the priority bandwidth.

These non-priority stations are referred to as “normal” stations. Normal video stations may or may not get video, depending on the available bandwidth.

Set Up Your Bandwidth Pools

Bandwidth pools enable you to control video usage for normal video users and priority video users. You can divide the bandwidth into three pools:

- **Audio pool**

  The audio pool contains bandwidth for all audio calls, including the audio-component of multimedia calls.

- **Normal video pool**

  The normal video pool contains bandwidth for the video portion of a call made by a normal (non-priority) video user. You can set this pool to be shared. When this pool is shared, audio-only calls are allowed to borrow bandwidth from this pool.

- **Priority video pool**

  The priority video pool contains bandwidth that is dedicated to priority video users only. Audio calls and normal video users are not allowed to borrow bandwidth from this pool. However, if all of the priority video pool bandwidth is currently in use, priority video users can borrow bandwidth from the normal video pool, if available.

Sample Scenarios

This section provides some examples of how you could specify the bandwidth settings for your network.

Example 1

In this example, you do not want to allocate any bandwidth for video. You want to configure the network to use IP audio. Figure 1 shows how you would configure the bandwidth pools for this example.

Table 1: Bandwidth Settings for Example 1

Total Bandwidth	Audio Bandwidth Pool	Priority Video Bandwidth Pool	Normal Video Bandwidth Pool	Share Normal Video Bandwidth Pool
3 Mb	3 Mb	0 Mb	0 Mb	No

Example 2

In this example, your network has enough bandwidth to support video for all Users simultaneously. Since all of your Users can get as much bandwidth as they need, there is no need to specify priority Users. There is only one pool of bandwidth to be shared by audio and multimedia calls. Audio will come from the normal video pool. Figure 2 shows how you would configure the bandwidth for this example.

Table 2: Bandwidth Settings for Example 2

Total Bandwidth	Audio Bandwidth Pool	Priority Bandwidth Pool	Normal Video Bandwidth Pool	Share Normal Video Bandwidth Pool
NoLimit	0 Mb	0 Mb	3 Mb	Yes

Example 3

In this example, you have bandwidth for video only, and you want to reserve some bandwidth for the CEO. All voice calls will be routed another way. You want to reserve half of your bandwidth (1.5 Mb) for priority users. If priority users need more than 50% of the bandwidth, they will be able to use the available bandwidth from the normal video pool. Audio will come from the normal video pool. Figure 3 shows how you would configure the bandwidth for this example.

Table 3: Bandwidth Settings for Example 3

Total Bandwidth	Audio Bandwidth Pool	Priority Video Bandwidth Pool	Normal Video Bandwidth Pool	Share Normal Video Bandwidth Pool
3 Mb	0 Mb	1.5 Mb	1.5 Mb	No

Example 4

In this example, you do not want to use too much bandwidth on audio. You want to reserve most of the bandwidth for video, but you want to allow a few audio calls to keep costs down. You have a small number priority users. Figure 4 shows how you would configure the bandwidth for this example.

Table 4: Bandwidth Settings for Example 4

Total Bandwidth	Audio Bandwidth Pool	Priority Video Bandwidth Pool	Normal Video Bandwidth Pool	Share Normal Video Bandwidth Pool
3 Mb	0.9 Mb	0.6 Mb	1.5 Mb	No

The settings in table will allow a few audio calls and one or two priority calls depending on the bit rate. After the audio pool runs out of bandwidth, the calls will be forced to take another route since the since the normal video bandwidth pool is not shared. If a priority call occurs when all of the priority video bandwidth is used, it will use any available bandwidth in the normal video bandwidth pool before using bandwidth from the audio bandwidth pool.

Example 5

In this example, you do not want to use any IP bandwidth for audio. You want to use IGAR for audio. All IP bandwidth will be used for video. Figure 5 shows how you would configure the bandwidth for this example.

Table 5: Bandwidth Settings for Example 5

Total Bandwidth	Audio Bandwidth Pool	Priority Video Bandwidth Pool	Normal Video Bandwidth Pool	Share Normal Video Bandwidth Pool
3 Mb	0 Mb	0 Mb	3 Mb	No

Since you have allocated no audio bandwidth, audio calls will fall over to the public-switched telephone network. However, multimedia calls will take audio bandwidth and video bandwidth from the normal video bandwidth pool.

Example 6

In this example, you want video only for the Polycom VSX systems in the boardroom and in the CEO's office. Also, this bandwidth must be available always. There are no normal video users. The extensions for the Polycom VSX systems are administered for priority video. Figure 6 shows how you would configure the bandwidth for this example.

Table 6: Bandwidth Settings for Example 6

Total Bandwidth	Audio Bandwidth Pool	Priority Video Bandwidth Pool	Normal Video Bandwidth Pool	Share Normal Video Bandwidth Pool
3 Mb	2.1 Mb	0.9 Mb	0 Mb	No

Example 7

In this example, the following conditions exist:

- You want to guarantee a certain audio bandwidth and video bandwidth.
- You do not want to share the normal video bandwidth pool because you have very strict limitations on the bandwidth.
- You do not want to exceed any of the provisioned pools.

Figure 7 shows how you would configure the bandwidth for this example.

Table 7: Bandwidth Settings for Example 7

Total Bandwidth	Audio Bandwidth Pool	Priority Video Bandwidth Pool	Normal Video Bandwidth Pool	Share Normal Video Bandwidth Pool
3 Mb	0.9 Mb	0 Mb	2.1 Mb	No

Example 8

In this example, the following conditions exist:

- You want to guarantee a certain audio bandwidth and video bandwidth.
- You do not want to share the normal video bandwidth pool because you have very strict limitations on the bandwidth. By not sharing the normal video bandwidth pool, you guarantee:
  - a minimum level of video bandwidth
  - audio-only calls cannot impact the normal video bandwidth pool
- You do not want to exceed any of the provisioned pools.
- You want to specify a proportion of priority video users.

Figure 8 shows how you would configure the bandwidth for this example.

Table 8: Bandwidth Settings for Example 8

Total Bandwidth	Audio Bandwidth Pool	Priority Video Bandwidth Pool	Normal Video Bandwidth Pool	Share Normal Video Bandwidth Pool
3 Mb	0.9 Mb	0.6 Mb	1.5 Mb	No

In this example, 600 Kbit is reserved for priority video. A priority video user will be able to use the normal video pool if the priority pool is all used and bandwidth exists in the normal video pool.

Example 9

In this example, the following conditions exist:

- You want to share the normal video bandwidth pool.
- You have no priority video users.

Figure 9 shows how you would configure the bandwidth for this example.

Table 9: Bandwidth Settings for Example 7

Total Bandwidth	Audio Bandwidth Pool	Priority Video Bandwidth Pool	Normal Video Bandwidth Pool	Share Normal Video Bandwidth Pool
3 Mb	0.9 Mb	0 Mb	2.1 Mb	Yes

Since there are no priority video users, the normal video bandwidth pool is the entire video bandwidth pool. With no priority users and the bandwidth being shared, all of the bandwidth could be used as audio.

Example 10

In this example, the following conditions exist:

- You want to guarantee a certain audio bandwidth and video bandwidth.
- You want to share the normal video bandwidth pool.
- You have priority video users.

Figure 10 shows how you would configure the bandwidth for this example.

Table 10: Bandwidth Settings for Example 7

Total Bandwidth	Audio Bandwidth Pool	Priority Video Bandwidth Pool	Normal Video Bandwidth Pool	Share Normal Video Bandwidth Pool
3 Mb	0.9 Mb	0.6 Mb	1.5 Mb	Yes

In this example, 600 Kbit of bandwidth is reserved for priority video users. Audio cannot use this bandwidth. The maximum available bandwidth for audio is 2.4 Mb. (In this case, there would be no normal video bandwidth available.) The maximum available bandwidth for priority video users is 2.1 Mb.

Chapter 2: Design and Deployment Checklist

Overview

The chapter provides a checklist that will help you design and deploy the Avaya Video Telephony Solution R5.2.

Note:

For the latest firmware video compatibility matrix, go to **www.avaya.com/support**. and access Video Telephony Solution.

Network and PBX-Network Requirements

Question 1: Has a multimedia QoS policy been designed and deployed?

☐ **Yes**.

☐ **No**. Avoid best effort treatment of video. Avaya IP Softphone, Avaya one-X Communicator, and all Polycom conferencing devices support QoS for video. See the checklist in section 11.0 of the white paper from Polycom Global Services titled “Supporting Real-time Traffic: Preparing Your IP Network for Video Conferencing.”

Question 2: Has a default enterprise Maximum Call Rate been selected?

Note:

Use **change ip-codec-set** and enable “Allow Direct IP Multimedia” on page 2 of the form. In Avaya Communication Manager 5.2, there are two options: Normal users and Priority users.

☐ **Yes**.

☐ **No**. Recommend initial deployment with Maximum Call Rate of 384 Kbps.

Note:

Keep in mind the following:

- Allow for 20% for IP protocol overheads.
- High definition room systems support call rates of 4 Mbps.

Question 3: Is inter-PBX network connectivity less than 150 ms end-to-end one-way delay and less than 1% packet loss at all times?

☐ **Yes**.

☐ **No**. Expect slower call establishment. Compared to audio-only calls, multimedia calls have a greater number of round-trip signaling messages by a factor of 5.

Question 4: Does the VPN connection for Avaya IP Softphone and Avaya one-X Communicator have less than 150 ms one-way delay to Avaya Communication Manager, is packet loss less than 1%, and is jitter less than 20 ms?

☐ **Yes**.

☐ **No**. Avaya IP Softphone and Avaya one-X Communicator do not support automatic bit rate downgrades on packet loss feedback, nor do they perform ping tests for video assessment. The user must reduce call rate and reattempt the call to achieve the best video experience for the network conditions. In worst-case conditions, users may experience video disablement by Avaya Communication Manager for the call duration due to excessive video update requests.

Question 5: Are there video call scenarios that would cross more than three Avaya Communication Manager servers?

Note that a limitation of the solution is that shuffling to direct-ip is blocked for Avaya Communication Manager servers that are pushing tandem trunk-to-trunk multimedia calls. Hairpinning is allowed.

☐ **Yes**. Administer additional trunks to minimize the use of tandem Avaya Communication Manager servers, thereby reducing video-update latency. Avoid the use of slow CPU servers (for example, S8700) in tandem scenarios, since video signaling across many Avaya Communication Manager servers is exponentially more expensive than audio-only calls.

☐ **No**.

Feature Interactions and Limitations

Question 1: Is Call Recording, Whisper Page, or Service Observing going to occur on video calls?

☐ **Yes**. Expect audio-only calls unless the ad-hoc video conferencing feature is enabled. Each of these features counts as an audio-only participant in the call. See Question 2: Are video endpoints involved in conference calls and ad-hoc video conferencing is not enabled? on page 20 and Question 3: Are multiple video endpoints (any more than two) involved in calls and insufficient ad-hoc video conferencing ports are available? on page 20.

☐ **No**.

Question 2: Are video endpoints involved in conference calls[1] and ad-hoc video conferencing is not enabled?[2]

☐ **Yes**. Expect audio-only calls, even when only two of the endpoints are video endpoints. To prevent this, enable ad-hoc video conferencing. There may be benefits to enabling ad-hoc video conferencing without any ad-hoc video conference bridges. For more information, see Question 3: Are multiple video endpoints (any more than two) involved in calls and insufficient ad-hoc video conferencing ports are available? on page 20

☐ **No**. For more information, see Question 3: Are multiple video endpoints (any more than two) involved in calls and insufficient ad-hoc video conferencing ports are available? on page 20.

Question 3: Are multiple video endpoints (any more than two) involved in calls and insufficient ad-hoc video conferencing ports are available?

☐ **Yes**. Expect audio-only calls. If there are no video ad-hoc video conferencing ports available, you only receive video if there are exactly two video parties on the call. If there are more than two video parties, no-one receives video, because there is no good rule for deciding which two parties should have it. If you have exactly two video-enabled parties, you can have as many audio-only parties as will fit and you will still get video.

Notes:

- A call over a video-enabled trunk counts as a video party, even if it is to an audio-only endpoint.
- A call over a non-video-enabled trunk counts as a non-video party, even if it's to a video endpoint.

1 Conference calls refer to calls with more than two participants.
2 The limitation described in this question case may not include calls to auxiliary devices over trunks (for example, using dedicated video conferencing devices).

Note:

It is important to note that this includes calls routed via IGAR, and may include failover trunks.

- A video-enabled station with a non-video endpoint registered to it (such as, a shared-control station with the video IPSP logged out) does not count as a video endpoint.
- A video station with video stopped or muted still counts as a video station.
- If you have video, and you add a video-enabled party, you lose video.
- If you drop all but two of your video-enabled parties, video returns.

☐ **No**.

Question 4: Is “transfer to MGC/RMX” being used for ad-hoc video conferencing?

☐ **Yes**. Avoid scenarios where a user attempts to transfer to a meeting room where tandem Avaya Communication Manager servers link the user to the Polycom MGC/RMX. Multiple Avaya Communication Manager shuffling (if allowed) may legitimately block the transfer. A reattempted transfer should succeed.

☐ **No**.

Question 5: Should a customer with a network of PBXs trunked together who will want to deploy ad-hoc video conferencing with Polycom RMXs in the future deploy those RMXs in a distributed manner?

☐ **Yes**. Ad-hoc video conferencing will require at least one Polycom RMX per active Avaya Communication Manager to support future ad-hoc video conferencing via the Conference button.

☐ **No**.

Question 6: Have additional media resources been allocated for Avaya Communication Manager servers that are used for tandem multimedia calls?

In a typical hub and spoke arrangement of Avaya Communication Managers, the core PABX that is doing the tandem calls between remote PABX systems should have additional media resources deployed as shuffling to direct-ip is blocked for multimedia calls.

☐ **Yes**.

☐ **No**. Expect higher utilization of media resources on tandem Avaya Communication Managers.

Avaya Communication Manager Global Administration

Question 1: Are the video capacities on system-parameters customer-options, page 2 configured correctly?

Maximum Video Capable H.323 Stations should be 1 x the number of single point Polycom VSX systems.

Maximum Video Capable IP Softphones should be equal to the number of video softphones.

Maximum Administered Ad-hoc Video Conferencing Ports should be based on the number of RMX systems and the maximum port count capability for the RMX systems.

☐ **Yes**.

☐ **No**.

Question 2: Are the fields on system-parameters customer-options, page 4 configured correctly?

"Enhanced Conferencing?" = **y**

"IP Trunks?" = **y**

"IP Stations?" = **y**

"ISDN-BRI Trunks?" = **y**

"ISDN-PRI?" = **y**

"Multimedia Call Handling (Basic)?" = **n**

"Multimedia Call Handling (Enhanced)?" = **n**

☐ **Yes**.

☐ **No**.

Question 3: Are the fields in ip-network-region, page 1 configured properly for all regions used by video endpoints?

"Intra-region IP-IP Direct Audio" = **y**

"Inter-region IP-IP Direct Audio" = **y**

Note:

For network regions containing third-party gatekeepers, these values must be set to **No** for direct audio because shuffling may not be supported by all third-party endpoints.

☐ **Yes**.

☐ **No**. Note the actual settings in this page and find out the customer's reasons/requirements for these options to be disabled. Video endpoints do not need to be shuffled to resume video. Third-party endpoints will support basic call setup only.

Question 4: Are the fields in ip-network-region, page 2 configured properly for all regions used by video endpoints?

H.323 SECURITY PROFILES must contain **any-auth** for Polycom VSX/HDX series devices to authenticate. **challenge** is used by Avaya IP Softphone & Avaya one-X Communicator. **pin-eke** is used by Polycom VSX/HDX series devices. **any-auth** encompasses both **challenge** and **pin-eke**.

☐ **Yes**.

☐ **No**. Expect registration failures.

Question 5: Is the ip-codec-set form configured properly?

Review all codec-sets used across the enterprise including the codec-sets used by media processors, trunks, and stations as well as inter-region codec sets. Has the enterprise selected a single version of G.711 across all Avaya Communication Manager servers globally?

☐ **Yes**.

☐ **No**. Simplify the codec-set administration by selecting one variant of G.711 across the entire network of Avaya Communication Manager servers. **A single variant can be used globally.** Otherwise expect codec mismatch errors and call drops between Avaya Communication Manager servers. Multimedia signaling uses H.245, which is more sensitive to codec administration than audio-only repeat-fast start signaling.

Question 6: Is the intra-region audio administration correct in the ip-codec-set form?

Review all IP codec-sets used across the enterprise including the IP codec-sets used by media processors, IP trunks, and IP stations.

Wide-band codecs (for example, SIREN series, G.722.1 series, and G.722-64k) should appear first and are supported for shuffled Polycom VSX calls only across a single Avaya Communication Manager.

G.711 should appear next.

Then follow with G.729/G.729A codec, etc.

☐ **Yes**.

☐ **No**.

Question 7: Is the inter-region audio administration correct in the ip-codec-set form?

Review all codec-sets used across the enterprise including the codec-sets used by media processors, IP trunks, and IP stations.

Are there bandwidth issues? If no, then re-use the one codec set also in use for intra-region.

If there are bandwidth issues, specify a low bandwidth codec first followed by one G.711 codec. If there are severe bandwidth issues, customers can choose to leave out G.711 and also ensure video is disabled.

☐ **Yes**.

☐ **No**.

Question 8: Is the audio administration for Polycom VSXs correct in the ip-codec-set form?

Review all codec-sets used across the enterprise including the codec-sets used by media processors, trunks, and stations.

If codec-sets used for stations include G.729, then a new network-region and codec must be defined for use by Polycom VSXs. VSX stations do not support G.729 but do support G.729A.

Note that media encryption is not supported by VSX stations.

☐ **Yes**.

☐ **No**. Expect call setup failure. This is a work around for a VSX signaling issue.

Question 9: Is the video administration correct in the ip-codec-set form?

Review page 2 of all the codec-sets to be used by video stations and video trunks.

Is “Allow Direct-IP Multimedia?” set to **yes**?

Is “Maximum Call Rate for Direct-IP Multimedia” set appropriately considering whether the codec-set is used for inter-region where there are bandwidth issues.?

☐ **Yes**.

☐ **No**. Expect audio only calls.

Question 10: Is ip-network-region inter-region video bandwidth management used across WAN links?

Ensure appropriate video total bandwidth limits on ip-network-region page 3 are set correctly.

☐ **Yes**.

☐ **No**. Expect low-quality video. Avaya recommends replacement of CAC via trunk-member counting with cumulative bandwidth management. Note that unlike audio, Avaya Communication Manger’s bandwidth management feature does not take into account the variable video headers. Allow 20% overheads. Best practice recommends video applications should consume no more than 35% of the total WAN bandwidth.

Question 11: Is video station administration correct in the station form?

First refer to this guide or the quick setup guide.

Ensure “IP Video?” is **yes**.

Ensure “IP Video Softphone?” is **yes**.

On page 2, ensure “Direct IP-IP Audio Connections?” is **yes**.

☐ **Yes**.

☐ **No**. Expect audio only calls.

Question 12: Is signaling group administration appropriate for video support?

Review the signaling groups used between Avaya Communication Managers, to Polycom MGCs/RMXs, and to SE200s. Also refer to this guide or the quick setup guide.

Ensure “IP Video?” is **yes**.

Ensure “Direct IP-IP Audio Connections?” is **yes**.

Ensure “Calls Share IP Signaling Connection?” is **No**, though this setting may be **Yes** between Avaya Communication Manager servers.

Does the network-region value correspond to an ip-codec-set that supports video?

☐ **Yes**.

☐ **No**. Expect audio only calls.

Question 13: Does the network-region value in the change signaling-group form correspond to an ip-codec-set that supports video?

☐ **Yes**.

☐ **No**. Expect audio only calls.

Question 14: Is DSCP tagging provisioned correctly?

Ensure that DSCP parameters are provisioned for the network region to which endpoints are registered.

For Avaya Communication Manager Release 4.0: Polycom VSX 8.5.3 onwards and Polycom MGC 8.0.1 onwards will automatically obtain DSCP parameters as configured in the network region. All other endpoints should have DSCP parameters set manually to the same values to which Avaya Communication Manager is set.

☐ **Yes**.

☐ **No**. This is not best practice.

Question 15: For shared control of IP sets, is the network region of the Avaya IP Softphone the same as the IP set?

Use the **change ip-network-map** command to ensure that the Avaya IP Softphone is mapped to the same network region as the IP set.

Note:

For shared control when using video, the only option supported is **via the server**. Do not try using the **via the phone (CTI)** option.

☐ **Yes**.

☐ **No**. Do not do this. This is not supported, so expect undefined results. When using shared control with video, the network region used for Avaya IP Softphone must match the network region used by the IP set. For Avaya Communication Manager Release 5.0 and later, this will not be a limitation.

Avaya Communication Manager Administration for Ad-hoc Video Conferencing

Question 1: Are the ad-hoc video conferencing capacities on system-parameters customer-options, page 2 configured correctly?

Ensure the “Maximum Administer Ad-hoc Video Conferencing Ports” is set to the number of ports available for Ad-hoc video conferencing.

☐ **Yes**.

☐ **No**.

Question 2: Has a Class of Service (COS) been assigned with “Ad-hoc Conferencing” enabled?

☐ **Yes**.

☐ **No**. Use the **change COS** command to enable Ad-hoc Video Conferencing.

Question 3: Has a video bridge been added using the add video-bridge command?

☐ **Yes**.

☐ **No**. Use the add video-bridge command to add Polycom MGC or Polycom RMX details for Ad-hoc video conferencing.

Avaya Communication Manager Administration for Polycom Multipoint Stations (VSX and HDX)

Question 1: Does each extension for a given multipoint endpoint have the same password configured on the station form?

For a multipoint station, each extension must have the same password. However, this password does not need to match the password for other multipoint stations.

☐ **Yes**.

☐ **No**. Use the **change station** command to set the “Security Code” entries to match. If these entries do not match, Avaya Communication Manager may reject registration by the station or confine it to one extension only.

Question 2: Has “Hunt-to Station” been configured to a circular hunt on the station form?

Configuring “Hunt-to Station” to a circular hunt enables Avaya Communication Manager to find the unused extension when dialing a multipoint station that is already in a call. This allows you to always call the main extension for the multipoint station.

☐ **Yes**.

☐ **No**. Use the **change station** command to set “Hunt-to Station” so that each station hunts to the next one, and the last station hunts to the first one.

Question 3: Has “Coverage” been configured on the station form?

The coverage feature has priority over the hunt-to feature and will interfere with it. The first call to the main Polycom VSX/HDX extension will succeed, but other calls will be busy (instead of hunting correctly). Setting "Station Hunt Before Coverage?" to "y" will also work but has system-wide consequences.

☐ **Yes**. Use the **change station** command and set “Coverage” to blank.

☐ **No**.

Avaya Communication Manager Administration for Polycom MGC Systems

Question 1: Polycom MGCs with multiple IP boards in conjunction with S87xx servers with multiple CLAN boards in regions require administration planning. Has this guide or the quick setup guide been used and understood?

☐ **Yes**.

☐ **No**. Complex signaling group and trunk group administration is required. Follow the rules in this guide and the quick setup guide. This solution offers a number of high availability options. CLAN board failures and IP board failures can be survivable. Incorrect administration can cause intermittent service.

Question 2: In Avaya Communication Manager Release 4.0, do signaling groups to Polycom MGCs have “Layer 3 Tests?” set to No?

☐ **Yes**.

☐ **No**. Expect signaling groups to go out of service (OOS).

Question 3: Is the outgoing trunk group to the Polycom MGC configured correctly in the change trunk-group form?

On Trunk group page 1, “Direction” must be **outgoing**.

On Trunk group page 1, “Outgoing Display” may be **y**. This is helpful for diagnostics.

On Trunk group page 2, “Disconnect Supervision – Out?” must be **y** to allow transfer to the MGC.

On Trunk group page 3, “Send Calling Number” must be set to allow the MGC to resolve calling party against the participant list on MGC conferences when pre-administered with participants.

☐ **Yes**.

☐ **No**. Expect trunk transfer failure. Expect wasted resources on the MGC.

Question 4: Is the incoming trunk group for the Polycom MGC configured correctly in the change trunk-group form?

On Trunk group page 1, “Direction” must be **incoming**.

On Trunk group page 2, “Disconnect Supervision – In?” must be **y** to allow transfer of MGC-initiated calls to other trunks.

☐ **Yes**.

☐ **No**. Expect trunk transfer failure.

Question 5: Is there only one incoming trunk group per Polycom MGC?

☐ **Yes**.

☐ **No**. Read this guide or the quick setup guide.

Question 6: Does the Polycom MGC have additional IP boards?

☐ **Yes**. For board redundancy, administer a second outgoing trunk group for the second to “nth” IP boards.

☐ **No**. Only one outgoing trunk group is required.

Question 7: Is the outgoing signaling group to the MGC configured correctly?

“LRQ Required?” must be **y**.

“Near end Listen Port” must be **1719**.

“Far end Listen Port” must be **1719**.

“Trunk Group for Channel Selection” must be clear.

☐ **Yes**.

☐ **No**. Expect call failures or intermittent call failures, or shuffling that shuts down video.

Question 8: Is the incoming signaling group to the Polycom MGC configured correctly?

"RRQ Required?" must be **y**.

"ARQ Required?" must be **y**.

"Near end Listen Port" must be **1720**.

"Far end Listen Port" must be **1720**.

"Trunk Group for Channel Selection" must be set to the trunk that uses the group.

☐ **Yes**.

☐ **No**. Expect call failures.

Question 9: If a Polycom MGC is to be used for six-party Ad-hoc video conferencing with Avaya Communication Manager, has the MGC been placed in a dedicated network region?

You must have:

- a dedicated network region for MGC use
- dedicated codec sets to infer the conference bit rates

Map the MGC to the new dedicated network region using the region field on the signaling groups connected to the MGC.

Ensure that you are using a codec set that reflects the correct conference bit rates for the MGC's network region.

Use the **change ip-network region** command to ensure that all other network regions have direct connectivity to the MGC's network region.

☐ **Yes**.

☐ **No**. Expect the MCU selection algorithms to make compromised decisions based on potentially incorrect inferred information from the codec-set conference bit rates.

Avaya Communication Manager Administration for Polycom RMX Systems

Question 1: Is a single, dual-direction trunk-group to the Polycom RMX configured correctly in the change trunk-group form?

On Trunk group page 1, “Direction” must be **both**.

On Trunk group page 1, “Outgoing Display” may be **y**. This is helpful for diagnostics.

On Trunk group page 2, “Disconnect Supervision – In?” must be **y** to allow transfer to the RMX.

On Trunk group page 2, “Disconnect Supervision – Out?” must be **y** to allow transfer to the RMX.

On Trunk group page 3, “Send Calling Number” must be set to allow the RMX to resolve calling party against the participant list on RMX conferences when pre-administered with participants.

☐ **Yes**.

☐ **No**. Expect trunk transfer failure. Expect wasted resources on the RMX.

Question 2: Is the signaling group to the Polycom RMX configured correctly?

“RRQ Required?” must be **y**.

“ARQ Required?” must be **y**.

“Near end Listen Port” must be **1720**.

“Far end Listen Port” must be **1720**.

“Trunk Group for Channel Selection” must be set to the trunk that uses the group.

☐ **Yes**.

☐ **No**. Expect call failures.

Question 3: In Avaya Communication Manager Release 4.x, do signaling groups to Polycom RMX have “Layer 3 Tests?” set to No?

☐ **Yes**.

☐ **No**. Expect signaling groups to go out of service (OOS).

Polycom MGC Configuration

Question 1: Does Network Service Properties have AVF?

Check that “Service Mode” is set to **Pseudo Gatekeeper – AVF** on the “Network Services Properties” H.323 tab.

☐ **Yes**.

☐ **No**. If this option is not available, install the Avaya version of the Polycom MGC Manager.

Question 2: Is H.245 tunneling enabled in the system.cfg file?

Check that **IP_BOARD_PARAMETERS H245_TUNNELING** is set to **YES** in the system.cfg file.

☐ **Yes**.

☐ **No**. Set this parameter to **YES**.

Question 3: Is G.729 disabled in the system.cfg file?

Check that **IP_AUDIO G729** is set to **NO** in the system.cfg file.

☐ **Yes**.

☐ **No**. You must set this parameter to **NO** to avoid call drops.

Question 4: Is wideband audio enabled in the system.cfg file?

In the system.cfg file, ensure that **AUDIO_PLUS_FREQUENCY** is set to **WB** (wideband). NOTE: The default value for this parameter is **MB** (medium band).

☐ **Yes**.

☐ **No**. Expect no wideband support by the MGC.

Question 5: For Polycom MGC version 8, is the Avaya mode enabled in the option flag in the system.cfg file?

☐ **Yes**.

☐ **No**. You must enable this parameter.

Question 6: Is the Polycom MGC registration refresh rate set to less than 60 seconds? (35 seconds is recommended.)

☐ **Yes**.

☐ **No**. In the MGC Manager, go to **<*MGC name*>-MCU Configuration-Network Services-IP-<*service name*>**. Find the H.323 tab, and ensure that “Refresh H.323 Registrations Every” is enabled and set to 35 seconds.

Question 7: Has 1*1 transcoding been set up?

Modify the desired conference room properties, and select the display option **1** on the Video Sources tab.

☐ **Yes**.

☐ **No**. MGC-MGC and MGC-RMX conference cascading may not display as expected.

Polycom RMX Configuration

Question 1: Is the Polycom RMX licensed for Avaya use?

Using the Polycom RMX web interface, go to **Administration>License Information**, and verify that Avaya is selected in “Polycom Partners.”

☐ **Yes**.

☐ **No**. Expect registration failure.

Question 2: Has the Polycom RMX system configuration been modified for use in the Avaya environment?

Using Setup menu>"System Configuration” tab, modify the following system configuration parameters:

- MCMS_PARAMETERS:
  - ENABLE_AUTO_EXTENSION = YES
  - MCU_DISPLAY_NAME = POLYCOM RMX-2000
  - CP_REGARD_TO_INCOMING_SETUP_RATE = NO
  - H323_FREE_VIDEO_RESOURCES = NO
  - NUMERIC_CONF_ID_LEN = 5
  - NUMERIC_CONF_ID_MAX_LEN = 8
  - NUMERIC_CONF_ID_MIN_LEN = 4
  - TERMINATE_CONF_AFTER_CHAIR_DROPPED = NO
- CS_MODULE_PARAMETERS:
  - H245_TUNNELING = YES

☐ **Yes**.

☐ **No**. Configuration not supported.

Question 3: Has a silence .wav file been installed?

Create a silence .wav file.

From the Polycom RMX web interface, click the note button (the right-most icon located below ivr services), and replace the music file with the silence .wav file you created.

☐ **Yes**.

☐ **No**. The RMX IVR audio for conference entry will be played when the first party joins the ad-hoc video conference.

Question 4: Has 1*1 transcoding been set up?

Modify the desired conference room properties, and select the display option **1** on the Video Sources tab.

☐ **Yes**.

☐ **No**. MGC-MGC and MGC-RMX conference cascading may not display as expected.

Polycom HDX/VSX System Configuration

Question 1: Are firewalls present between the Polycom VSX/HDX and the Avaya Communication Manager?

☐ **Yes**. Ensure H.245 port range 59000-59200 is open.

☐ **No**.

Question 2: Does the Polycom VSX Options page have “Multipoint” or “Multipoint Trial” enabled?

☐ **Yes**. On the Avaya Communication Manager, ensure that ***x*** (where ***x*** depends on the VSX type) consecutive stations are administered with the same password in a circular station hunt group. Refer to this guide or the quick setup guide.

☐ **No**.

Question 3: Is the “Avaya option” enabled on the Polycom VSX Options page?

☐ **Yes**.

☐ **No**. Install the new options key that will enable Avaya options.

Question 4: If H.239 is desired, is the H.239 option field enabled?

On VSX System->Admin Settings->Network->Call Preference, set **Enable H_239**.

☐ **Yes**.

☐ **No**. Dual video (people and content) will not work.

Avaya one-X Communicator

Question 1: Did you install the USB camera with the latest drivers and verify that the camera is working?

Verify the camera works using the software that was installed with the camera (for example, use Logitech QuickCapture for Logitech cameras).

☐ **Yes**.

☐ **No**.

Question 2: Did you update the PC with the latest software?

This is required for best performance. This includes video card drivers (VGA drivers) and Microsoft DirectX.

☐ **Yes**.

☐ **No**. Expect flickering video.

Question 3: Have you ensured that Avaya one-X Communicator is installed with video?

Note:

Video is only supported when you are using one-X Communicator in H.323 mode and without the Citrix feature.

When you purchase one-X Communicator, video is an optionally-licensed feature. It is also important to note that you must install and configure your Web camera before installing one-X Communicator. When you install one-X Communicator, you must select the **Video Integration** checkbox on the **Protocol and Feature Selection** dialog of the one-X Communicator installation wizard.

☐ **Yes**.

☐ **No**.

Question 4: Did you configure the Avaya one X Communicator Login settings for video?

After you install one-X Communicator is installed, you must perform an additional configuration step to enable video. From the one-X Communicator **Login** screen, you must navigate to **Settings** > **General Settings** > **Phone**. On the **Phone** panel, select the **Enable Video Calls** checkbox.

☐ **Yes**.

☐ **No**.

Question 5: Did you verify video registration after logging into one-X Communicator?

Verify that the video window is open and local video is displayed.

☐ **Yes**.

☐ **No**.

Avaya one-X Communicator Performance Issues

Question 1: Are there video issues?

Check the **Video Statistics** dialog. Check the information on all the tabs in the dialog, such as:

Status: The current statistics of the video.

Capabilities: The codec sets that one-X Communicator currently supports.

Signaling: The current signaling with the Avaya Communication Manager.

Question 2: If there are video issues, have you provided log files?

Logs files are located in:

```
C:\Documents and Settings\<username>\Application Data\Avaya\Avaya
one-X Communicator \Log Files\*
```

and:

```
C:\Documents and Settings\<username>\ Application Data\Polycom\
Video.vg2
```

Zip these files and send them to your Avaya Support Representative.

Question 3. Is the local view displaying black video?

Unplug your USB camera, wait 5 seconds, and then plug it back in again. If the local view is still displayed in black, close the video, then open it again in using the **Video Settings** dialog.

Priority Bandwidth Management

Question 1: Has a COS been assigned with “Priority IP Video” enabled?

☐ **Yes**.

☐ **No**. Use **change cos** and enable **Priority IP Video**.

Question 2: Have inter-region video limits been set for normal and priority callers?

☐ **Yes**.

☐ **No**. Use **change ip-network-region** and allocate priority video bandwidth across WANs on page 3 of the form.

Question 3: Has the Maximum Call Rate for Priority Direct-IP Multimedia been set?

☐ **Yes**.

☐ **No**. Use **change ip-codec-set** and set appropriate the maximum call rates for priority and normal video users on page 2 of the form.

Question 4: Do Polycom MGC trunks need access to priority bandwidth pools across the Avaya Communication Manager network for MGC dialout scenarios?

☐ **Yes**. Set the “Priority Video” field to **yes** on the MGC signaling groups.

☐ **No**.

SIP Administration (Global)

Important:
SIP video devices configured as off-pbx-stations are not officially supported on Avaya Communicator Manager 5.2. Avaya one-X Communicator with SIP video support will be available in a future Communication Manager release. Polycom devices are not currently supported with SIP features enabled. Other third party SIP devices must have achieved DevConnect video certification to receive any support with video enabled.

Question 1: Is Avaya Communication Manager licensed for SIP video?

Verify that the fields have been configured correctly on page 4 of the system-parameters customer-options form. "Multimedia IP SIP Trunking?" must be set to "y."

☐ **Yes**.

☐ **No**. SIP video calls are not possible without the correct license. Installation of the license will enable the "IP Video" field on the SIP signaling group form.

Question 2: Are the video capacities configured appropriately on the system-parameters customer-options form, page 2?

“Maximum Video Capable Stations” should include H.323 and SIP video extensions. The following equation is a useful starting point:

```
Maximum Video Capable Stations =

<Number of Single Point VSXs> + <3 x Number of Multipoint VSXs> +
  <Number of H.323 and SIP video users>
```

For multipoint HDXs, the equation remains the same. However, it is important to note that each HDX system can be three stations for "Multipoint Plus Four" and seven stations for "Multipoint Plus Eight" multipoint licensed options for the HDX9004. The HDX9002 only has "Multipoint Plus Four" as an option. For more information, see Procedure 1: Determine the Maximum Number of Video-Capable H.323 Stations Supported on page 63.

☐ **Yes**.

☐ **No**. Video calls will be audio only if a signaling group is used without Direct IP-IP Audio Connections allowed.

Question 3: Is the authoritative domain for the IP network region in use set to match the SIP domain configured on the Avaya SIP Enablement Services (SES) server?

"Authoritative Domain" on page 1 of the ip-network-region form should be set to **yoursipdomain.com**.

- ☐ **Yes**.
- ☐ **No**. Expect "403 forbidden" denial messages, preventing call setup.

SIP Trunk Administration

Important:
SIP video devices configured as off-pbx-stations are not officially supported on Avaya Communicator Manager 5.2. Avaya one-X Communicator with SIP video support will be available in future a Communication Manager release. Polycom devices are not currently supported with SIP features enabled. Other third party SIP devices must have achieved DevConnect video certification to receive any support with video enabled.

Question 1: Is the SIP signaling group in use configured to allow video calls?

Verify that the fields have been configured correctly on page 1 of the signaling-group form. "IP Video?" must be set to "y."

☐ **Yes**.

☐ **No**. Video calls be audio only if a signaling group is used without IP Video allowed.

Question 2: Is the SIP signaling group configured to allow direct IP connections?

Verify that the fields have been configured correctly on page 1 of the signaling-group form. "Direct IP-IP Audio Connections?" must be set to "y."

☐ **Yes**.

☐ **No**. Video calls will be auto only if a signaling group is used without IP Video allowed.

SIP Station Administration (OPTIM)

Question 1: Is the IP station configured to use video?

Verify that the fields have been configured correctly on page 1 of the station form. "IP Video?" must be set to "y."

☐ **Yes**.

☐ **No**. Expect no video media if video is disabled for the station.

Question 2: Is the IP station configured to use direct media?

Verify that the fields have been configured correctly on page 2 of the station form. "Direct IP-IP Audio Connections?" must be set to "y."

☐ **Yes**.

☐ **No**. Expect no video media if direct media is disabled for a station.

Question 3: Is the station type correct for the SIP endpoint being administered?

Verify that the fields have been configured correctly on page 1 of the station form. "Type" must be set to "4620SIP" or "96xx."

For Avaya endpoints, ensure that the set type matches. All OPTIM video endpoints should use the "4620SIP" station type.

☐ **Yes**.

☐ **No**. An incorrect set type can cause registration failure or call setup failure.

Question 4: Is the OPTIM call limit configured to allow the number of simultaneous call appearances required by the endpoint?

Verify that the fields have been configured correctly on page 2 of the off-pbx-telephone station-mapping form. "Call Limit" should be set to the number of extensions/line appearances.

☐ **Yes**.

☐ **No**. Certain station features may be unavailable, or multipoint capabilities may not work as expected.

SIP Limitations

Question 1: In a mixed H.323/SIP environment, are all H.323 MCUs the supported RMX platform?

Verify that all H.323 bridges accessible to SIP video users are not MGCs.

☐ **Yes**.

☐ **No**. SIP video users will not receive video when dialing into an H.323 MGC. Upgrading to the Polycom RMX bridge will enable video for SIP users.

Question 2: Is the video routing feature set to prefer only H.323 trunks and not use SIP trunks with a multimedia bearer capability?

Verify that all route patterns containing SIP video trunks do not rely on the multimedia bearer capability being set.

☐ **Yes**.

☐ **No**. Multimedia bearer capability is not set for SIP video calls. As a result, SIP video calls will route as audio only.

Question 3: Is priority video enabled on a SIP signaling group, and is the bandwidth allocated from the priority pool as expected?

Verify that the signaling groups at either end of the SIP trunk have priority video enabled if it desired to use priority bandwidth. Separate sub-domain names may be used to separate priority and normal users.

☐ **Yes**.

☐ **No**. SIP currently has no means to signal a priority video call over a trunk. A system that receives a call on a priority trunk will always be allocated bandwidth from the priority pool.

Question 4: Do all non-Avaya SIP video endpoints have DevConnect certification?

Verify that all non-Avaya SIP video enpoints have DevConnect certification. Communicator Manager places specific requirements on SIP endpoints to ensure seamless inter-working between SIP/H.323 with full access to enterprise features.

☐ **Yes**.

☐ **No**. Avaya recommends that users of uncertified SIP video equipment disable video on the device when calling into the Avaya video telephony solution.

Question 5: Is media encryption enabled for a network region containing SIP endpoints?

SRTP media encryption is not supported simultaneously with SIP video. Video is disabled for any calls that require audio encryption. If video is required without security, then ensure that users are assigned a codec-set without SRTP media encryption using ip-network-region segmentation.

☐ **Yes**.

☐ **No**.

Additional Information

For more information about connecting a Polycom MGC to a trunked SIP video device, see MGC Limitations on page 103.

Chapter 3: Setting Up Video Endpoints

This chapter contains the following sections:

- The installation and configuration steps for a number of video endpoints:
  - Configure a Station Endpoint for Avaya IP Softphone Release 6.0 and Video Integrator
  - Configure a Station Endpoint for Avaya one-X™ Communicator with H.323
  - Configure Polycom VSX/HDX Series Video Conferencing Systems and V500/V700 Video Calling Systems
  - Configure a Polycom RMX Series Video Conferencing Bridge Platform
  - Configure Ad-hoc Video Conferencing for a Polycom RMX Series Video Conferencing Bridge Platform
  - Configure a Polycom MGC-25 Video Conferencing Bridge Platform for an Avaya S8300 Server
  - Configure Polycom MGC Video Conferencing Bridge Platforms with Avaya S8500 and S87xx Server
  - Configure a SE200 Gatekeeper
  - Configure a Tandberg Centric 1700 MXP
  - Configure a Tandberg Centric 150 MXP
  - Configure Unauthenticated H.323 Endpoints
  - Configure a Direct Routing Gatekeeper
- The configuration steps for enabling Ad-hoc video conferencing on a system running Avaya Communication Manager Release 5.2. For more information, see Configure Video Trunks between Two Avaya Communication Manager Systems.
- The steps involved in monitoring the status of video bandwidth usage. For more information, see Monitor the Status of Video Bandwidth Usage.
- A description of the logic that Avaya Communication Manager uses to selects bridges. For more information, see Communication Manager Selection of Video Bridge.
- A list of the issues involved in considering ad-hoc licenses. For more information, see Ad-hoc Licensing Considerations.

Required Administration

Before administering any video endpoints on your system, you must perform the following procedures:

- configure IP codec sets
- configure IP network regions

Note:

Review the information in Avaya Communication Manager Global Administration on page 22 before performing the procedures in this section.

Configure IP Codec Sets

To configure the IP codec sets that you want to use for video:

1. Use the **change ip-codec-set *x*** command (where ***x*** is the chosen IP codec set) to access the IP Codec Set form.
2. Define the codecs. The following codecs are recommended:
   - SIREN14-48K (1 fpp, 20 ms)
     SIREN14-48K are wideband codecs. Since most Polycom systems are not configured for stereo, it is not recommended to use a stereo SIREN codec as a default.
   - G.722-64K (2fpp, 20 ms)
     G.722-64K are wideband codecs. These codecs allow wideband with video endpoints that do not support SIREN codecs. G.722-64K codecs are required if you are using VSX systems in mixed H.320/H.323 environments. Be sure to place this codec above the other non-Siren audio codecs.
   - G.722.1-32K (1 fpp, 20 ms)
     G.722.1-32K are wideband codecs. These codecs allow wideband with video endpoints that do not support SIREN codecs.
   - G.729A (no silence suppression, 2 fpp, 20 ms)
     Polycom systems do not support all variants of G.729 codecs. If you want to use G.729, you must specify G.729A. If you specify G.729, no audio problems arise. All variants of G.729 codecs are narrowband codecs.

   Note:

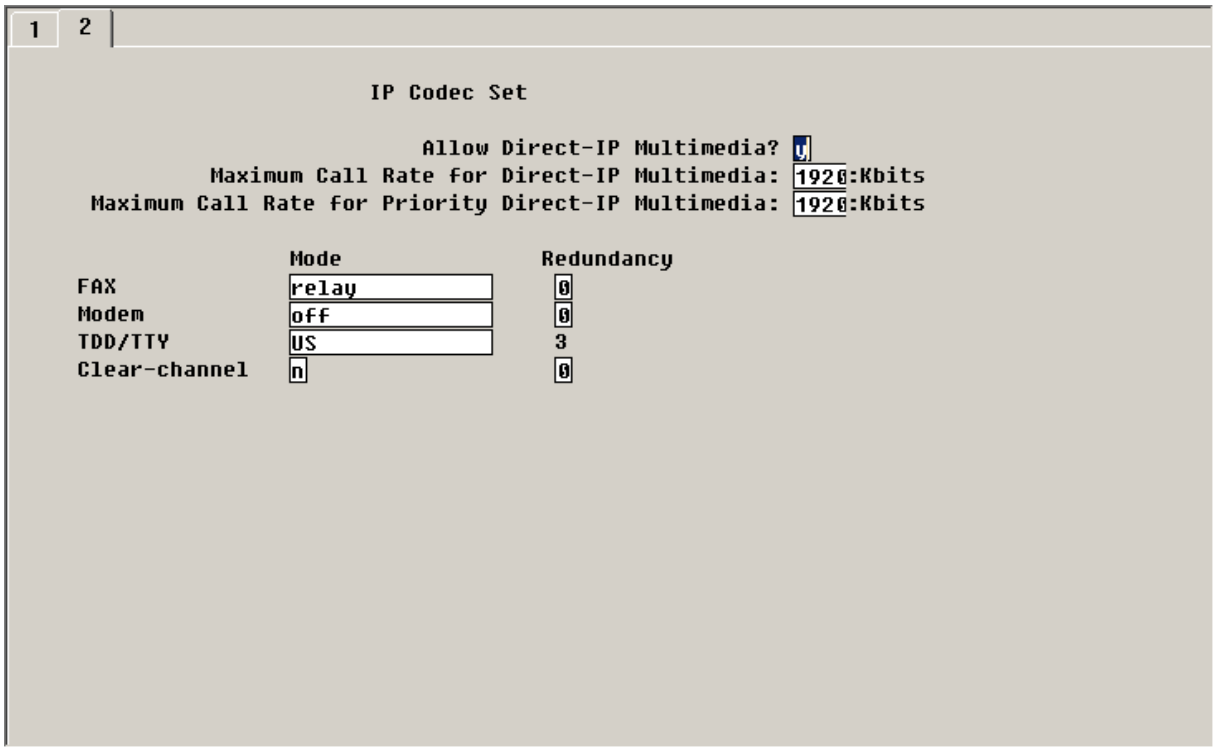
   Keep in mind the following information:

   - Wideband codecs should appear before narrowband codecs in the codec set. If you are using VSX systems in mixed H.320/H.323 environments, place the **G.722-64K** audio codec above the other non-Siren audio codecs.

- G.711 codecs are recommended for Avaya Meeting Exchange 5.1. Avaya Meeting Exchange 5.1 does not support wideband codecs.

3. Go to page 2 of the form.

Figure 1: Example of Page 2 of the IP Codec Set Form



4. Set **Allow Direct-IP Multimedia** to **y**.
5. Set **Maximum Call Rate for Direct-IP Multimedia**. The range is 64 Kbits through 15360 Kbits (in increments of 64 Kbits). 384 Kbits is recommended.

   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.
6. Set **Maximum Call Rate for Priority Direct-IP Multimedia**. The range is 64 Kbits through 15360 Kbits (in increments of 64 Kbits). 384 Kbits is recommended.

   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.
7. Repeat Steps 1 through 6 for each IP codec set that will be used for video.

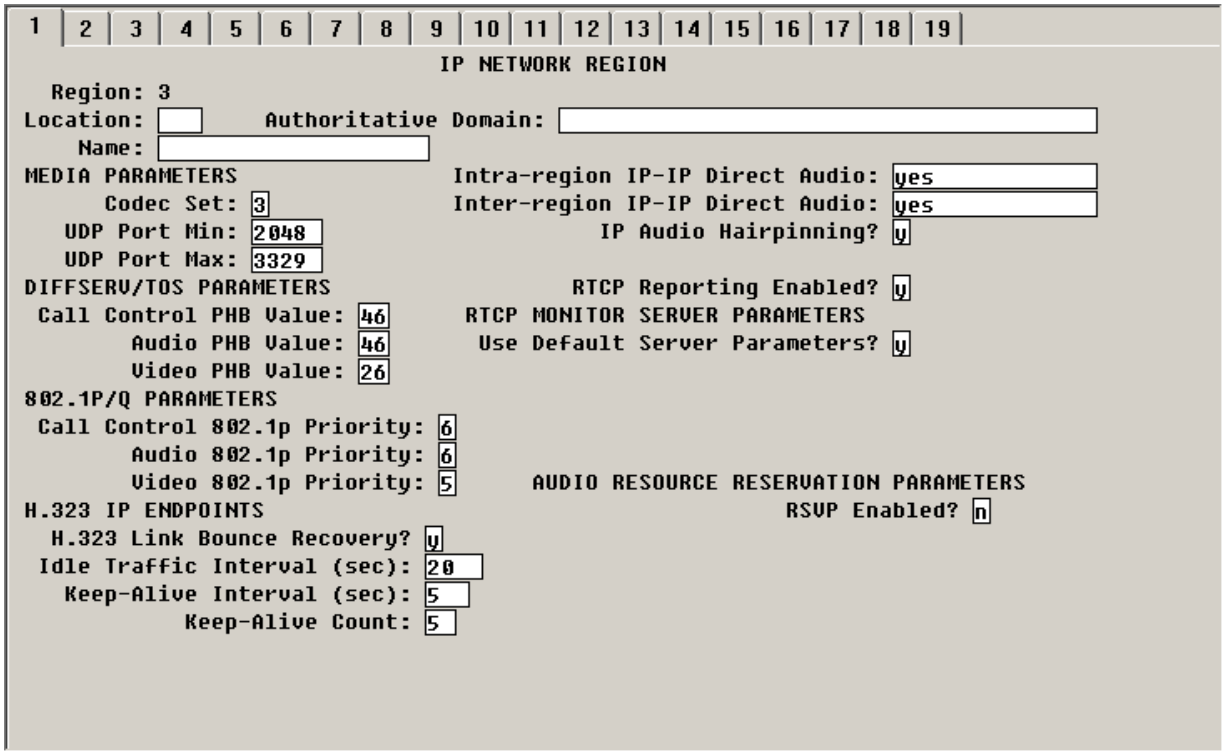
Configure IP Network Regions

To configure the IP network regions:

1. Use the **change ip-network-region *x*** command (where ***x*** is the chosen IP network region) to access the IP Network Region form for the specified region.

   The IP Network Region form appears.

Figure 2: Example of Page 1 of the IP Network Region Form



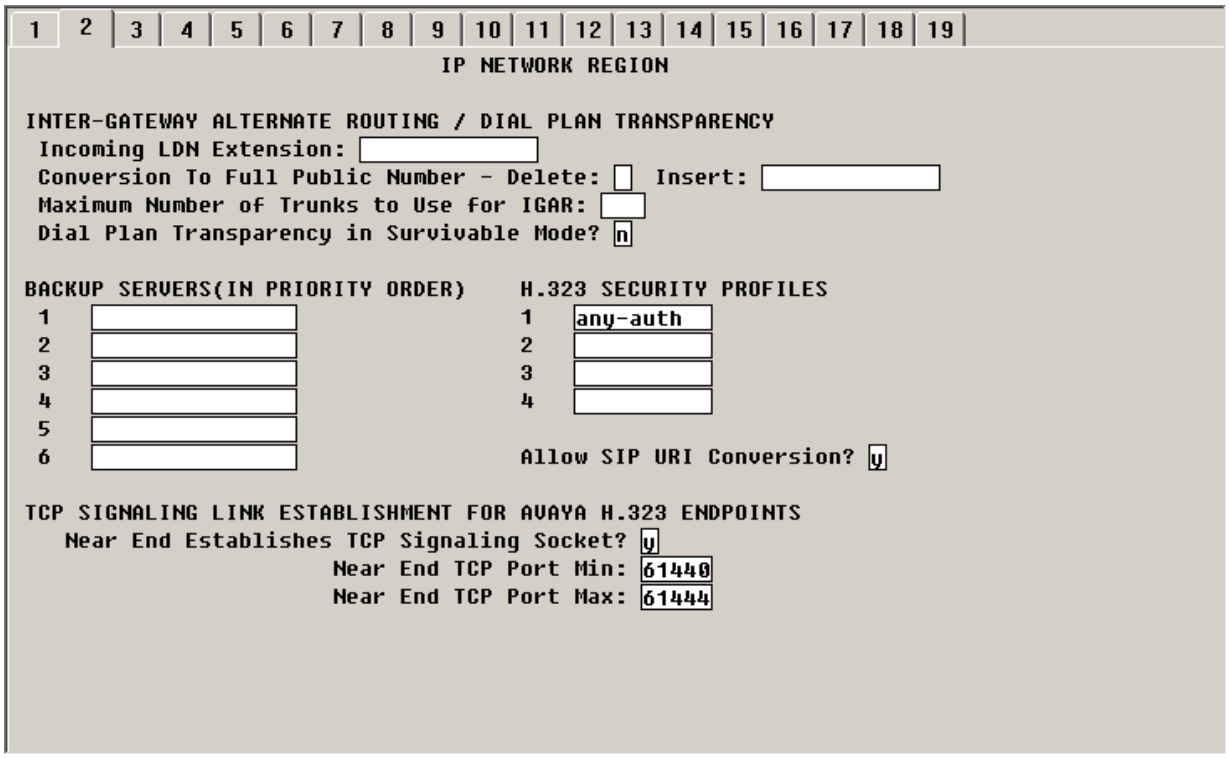
2. Set **Intra-region IP-IP Direct Audio** to **yes**.
3. Set **Inter-region IP-IP Direct Audio** to **yes**.

   Note:

   Shuffling is recommended. However, you can set shuffling to **no**, and video calls will work properly.

4. Go to page 2 of the form.

Figure 3: Example of Page 2 of the IP Network Region Form



5. Set **Security Procedures 1** to **any-auth**.
6. Go to page 3 of the form.
7. Set **codec set** to the codec set you defined in Procedure 2.
8. Set **Video Norm** to the amount of bandwidth that you want to allocate for the normal video pool to each IP network region.
9. Set **Video Prio** to the amount of bandwidth that you want to allocate for the priority video pool to each IP network region.
10. Set **Video Shr**. Specify whether the normal video pool can be shared with the audio pool for each link between IP network regions (**y** or **n**).
11. Repeat Steps 1 through 10 for each IP network region that will be used for video in this system.

Configure a Station Endpoint for Avaya IP Softphone Release 6.0 and Video Integrator

This section describes how to enable video calls for a desktop user.

Note:

Users must install Avaya IP Softphone Release 6.0 and Video Integrator on their PCs before they can handle video calls from their desktops.

Checklist

When setting up video calls for a desktop, you will need to know the following information:

- the station number of the desktop user
- the IP codec sets you want to use
- the IP network regions you want use

Configuration Procedures

To configure a station to use Avaya IP Softphone Release 6.0 and Video Integrator, you must perform the following steps:

1. Determine the maximum number of video-capable Avaya IP Softphone endpoints your voice system supports.
2. Configure the Class of Service if you want to use priority video calling.
3. Add a new station or modify an existing station that will use Avaya IP Softphone for video.

Procedure 1: Determine the Maximum Number of Video-Capable Avaya IP Softphone Endpoints Supported

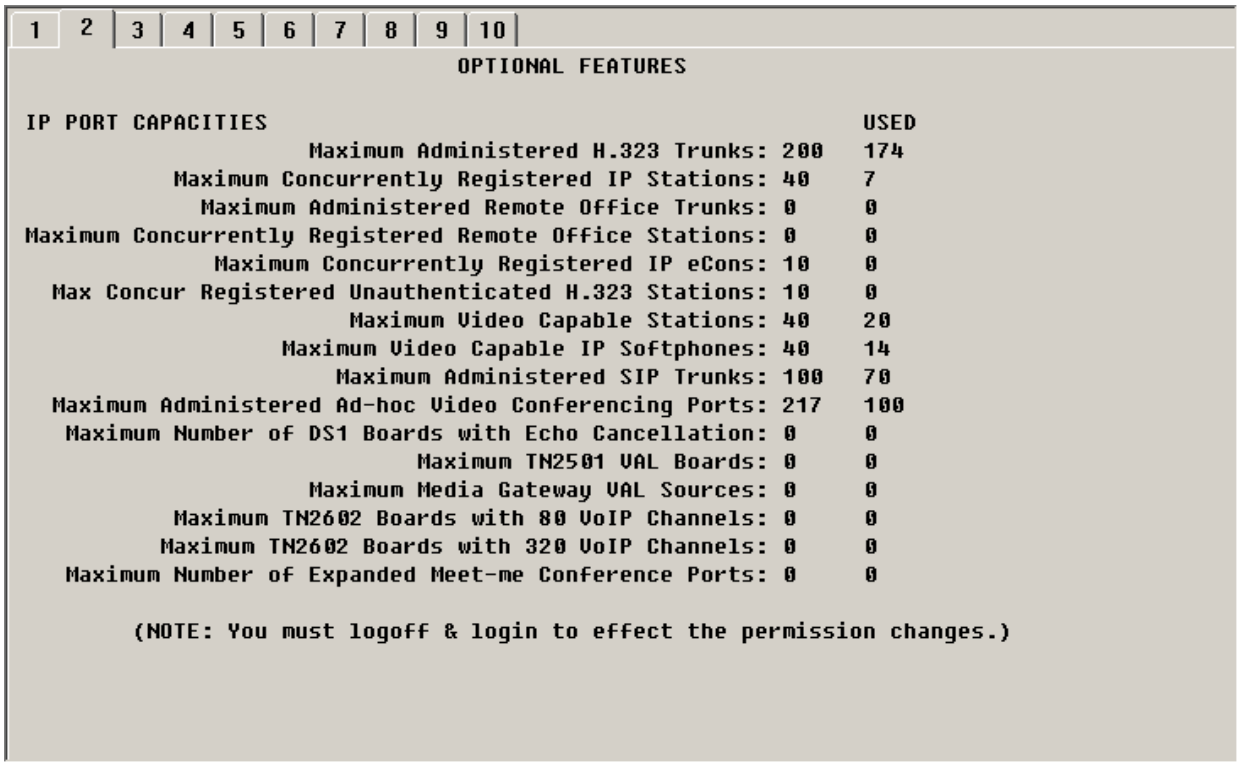
To determine the maximum number of video-capable Avaya IP Softphone endpoints your voice system supports:

1. Use the **display system-parameters customer-options** command to access the Optional Features form.
2. On page 2 of the form, verify the **Maximum Video Capable IP Softphones**. This number is provided by the RFA license file.

   Note:

   To provide video softphone capability, you must have at least this number of Avaya IP Softphone licenses. Page 10 of this form displays the number of Avaya IP Softphone licenses you have.

Figure 4: Example of Page 2 of the Optional Features Form



```
1  2  3  4  5  6  7  8  9  10

                              OPTIONAL FEATURES

IP PORT CAPACITIES                                          USED
                     Maximum Administered H.323 Trunks: 200   174
          Maximum Concurrently Registered IP Stations: 40    7
            Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
             Maximum Concurrently Registered IP eCons: 10    0
  Max Concur Registered Unauthenticated H.323 Stations: 10    0
                       Maximum Video Capable Stations: 40    20
                   Maximum Video Capable IP Softphones: 40    14
                      Maximum Administered SIP Trunks: 100   70
  Maximum Administered Ad-hoc Video Conferencing Ports: 217   100
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                            Maximum TN2501 VAL Boards: 0     0
                   Maximum Media Gateway VAL Sources: 0     0
          Maximum TN2602 Boards with 80 VoIP Channels: 0     0
         Maximum TN2602 Boards with 320 VoIP Channels: 0     0
   Maximum Number of Expanded Meet-me Conference Ports: 0     0

       (NOTE: You must logoff & login to effect the permission changes.)
```

In this example, the system can have a maximum of 40 video-enabled Avaya IP Softphone endpoints. Currently, 14 video-capable Avaya IP Softphone endpoints are being used.

Procedure 2: Configure Class of Service

Perform this procedure if you want to allow priority video calling.

To configure the Class of Service:

1. Use the **change cos** command to access the Class of Service form.
2. Go to page 2 of the form.
3. Set **Priority Video Calling** for the appropriate COS levels.

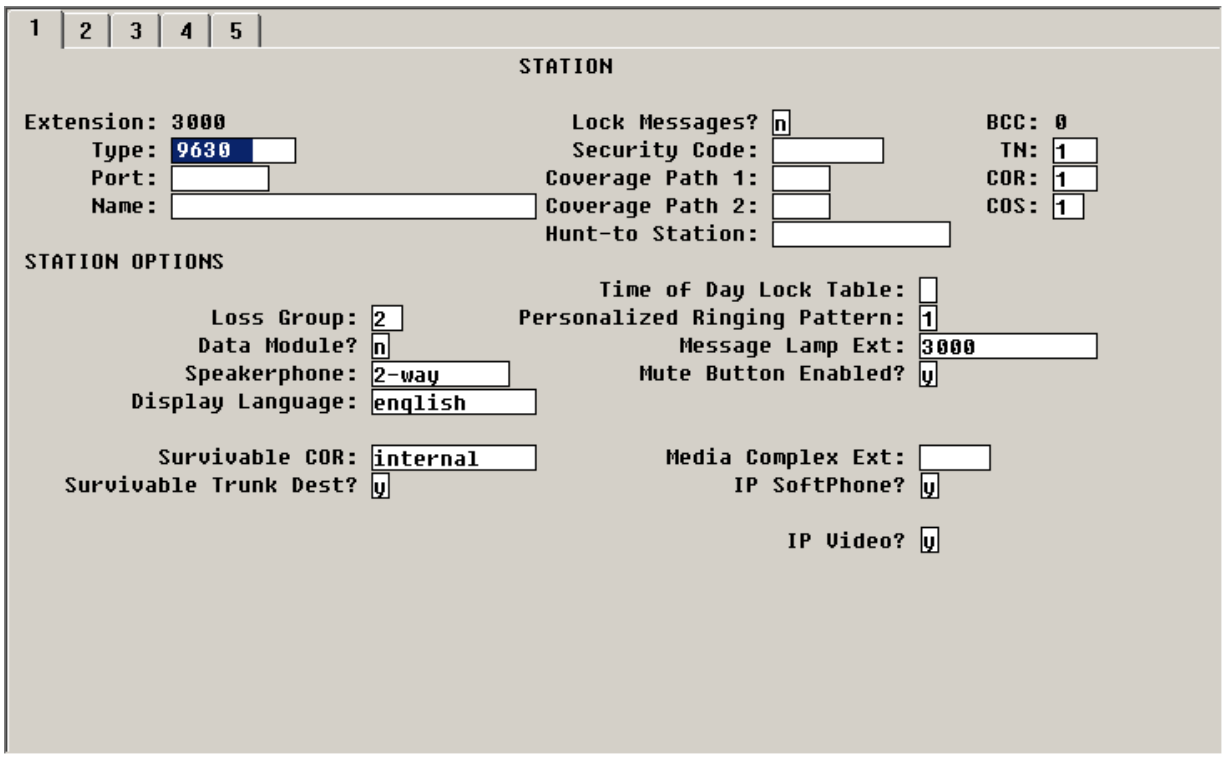
Procedure 3: Add a Video-Enabled Avaya IP Softphone Station

To add a video-enabled Avaya IP Softphone station:

1. Perform one of the following steps:
   - If you want to add a new station that will use Avaya IP Softphone, use the **add station** command.
   - If you want to modify an existing station that will use Avaya IP Softphone, use the **change station *xxxx*** (where ***xxxx*** is the number of the station you want to modify) command.

   The Station form appears.

Figure 5: Example of Page 1 of the Station Form



2. Enter the appropriate information for this station.
3. Set **IP Softphone** to **y**.
4. Set **IP Video Softphone** to **y**.
5. 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 Procedure 2.)
6. Repeat Steps 1 through 5 for each video-enabled Avaya IP Softphone endpoint you want to configure.

Configure a Station Endpoint for Avaya one-X™ Communicator with H.323

Avaya one-X Communicator can use either the H.323 or SIP protocol. When an Installation Engineer installs one-X Communicator, they make the choice between H.323 and SIP. This section describes how to enable video calls for a desktop user using the H.323 protocol. Avaya aim to support the SIP protocol in a future release of their video telephony solution.

Before you begin, it is important to verify that you have valid licenses for one-X Communicator. Video is an optional feature in Avaya one-X Communicator. In addition, Users must install Avaya one-X Communicator on their PCs before they can handle video calls from their desktops.

Checklist

When setting up video calls for a desktop, you will need to know the following information:

- the station number of the desktop user
- the IP codec sets you want to use
- the IP network regions you want use

Configuration Procedures

To configure a station to use Avaya one-X™ Communicator, you must perform the following steps:

1. Determine the maximum number of video-capable endpoints your voice system supports.
2. Configure the Class of Service if you want to use priority video calling.
3. Add a new station or modify an existing station that will use Avaya one-X Communicator for video.

Procedure 1: Determine the Maximum Number of Video-Capable Endpoints Supported

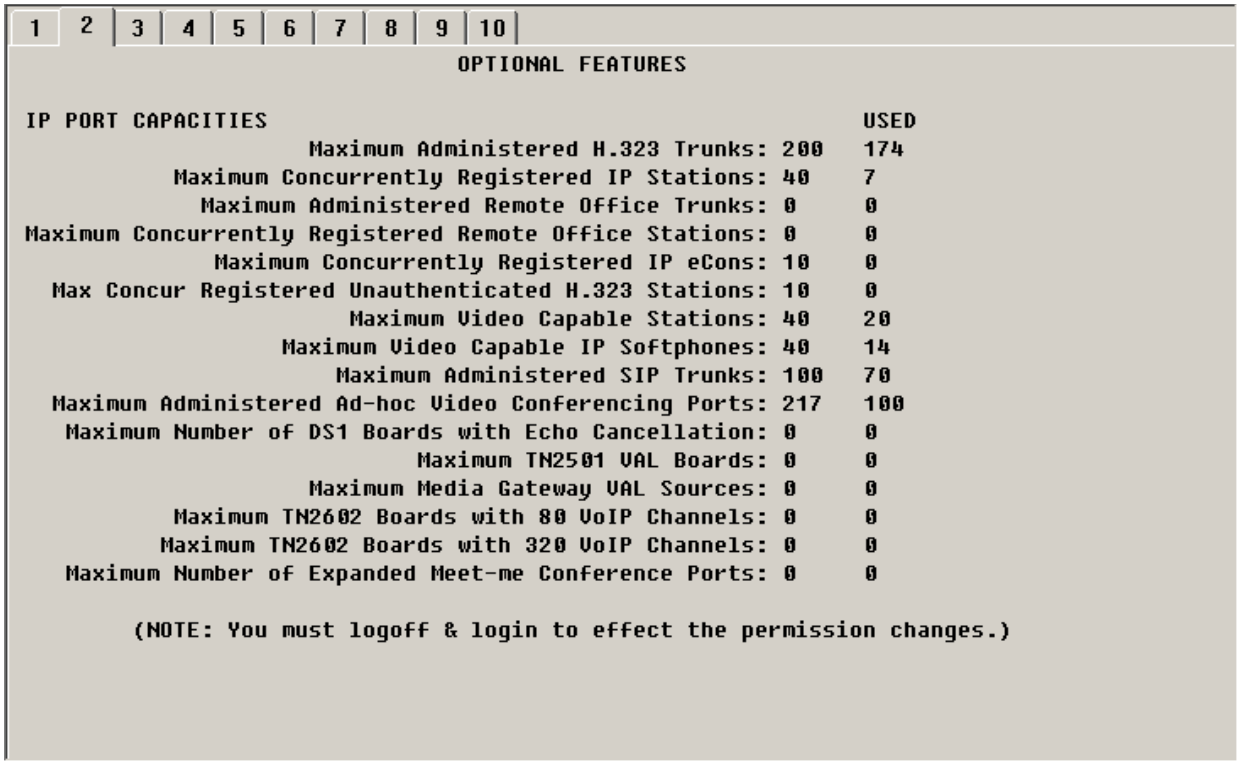
To determine the maximum number of video-capable endpoints your voice system supports:

1. Use the **display system-parameters customer-options** command to access the Optional Features form.
2. On page 2 of the form, verify the **Maximum Video Capable IP Softphones**. This number is provided by the RFA license file.

   Note:

   Avaya one-X Communicator uses the same pool of video licenses counted by the **Maximum Video Capable IP Softphones** parameter. To provide video softphone capability, you must have at least this number of Avaya one-X Communicator licenses. Page 10 of this form displays the number of Avaya one-X Communicator licenses you have.

Figure 6: Example of Page 2 of the Optional Features Form



1 2 3 4 5 6 7 8 9 10

OPTIONAL FEATURES

IP PORT CAPACITIES	USED
Maximum Administered H.323 Trunks: 200	174
Maximum Concurrently Registered IP Stations: 40	7
Maximum Administered Remote Office Trunks: 0	0
Maximum Concurrently Registered Remote Office Stations: 0	0
Maximum Concurrently Registered IP eCons: 10	0
Max Concur Registered Unauthenticated H.323 Stations: 10	0
Maximum Video Capable Stations: 40	20
Maximum Video Capable IP Softphones: 40	14
Maximum Administered SIP Trunks: 100	70
Maximum Administered Ad-hoc Video Conferencing Ports: 217	100
Maximum Number of DS1 Boards with Echo Cancellation: 0	0
Maximum TN2501 VAL Boards: 0	0
Maximum Media Gateway VAL Sources: 0	0
Maximum TN2602 Boards with 80 VoIP Channels: 0	0
Maximum TN2602 Boards with 320 VoIP Channels: 0	0
Maximum Number of Expanded Meet-me Conference Ports: 0	0

(NOTE: You must logoff & login to effect the permission changes.)

In this example, the system can have a maximum of 40 video-enabled Avaya one-X Communicator endpoints. Currently, 14 video-capable Avaya one-X Communicator endpoints are being used.

Procedure 2: Configure Class of Service

Perform this procedure if you want to allow priority video calling.

To configure the Class of Service:

1. Use the **change cos** command to access the Class of Service form.
2. Go to page 2 of the form.
3. Set **Priority Video Calling** for the appropriate COS levels.

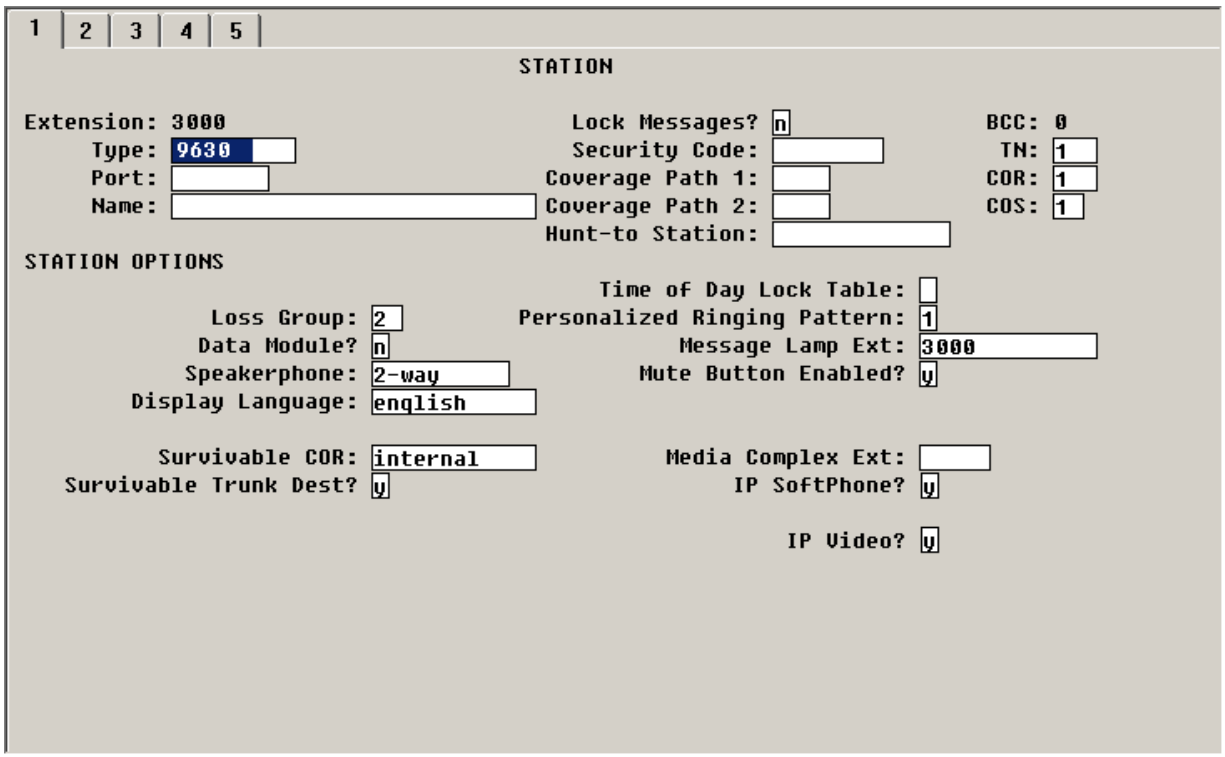
Procedure 3: Add a Video-Enabled Avaya one-X Communicator Station

To add a video-enabled Avaya one-X Communicator station:

1. Perform one of the following steps:
   - If you want to add a new station that will use Avaya one-X Communicator, use the **add station** command.
   - If you want to modify an existing station that will use Avaya one-X Communicator, use the **change station *xxxx*** (where ***xxxx*** is the number of the station you want to modify) command.

   The Station form appears.

Figure 7: Example of Page 1 of the Station Form



2. Enter the appropriate information for this station.
3. Set **IP Softphone** to **y**.
4. Set **IP Video** to **y**.
5. 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 Procedure 2.)
6. Repeat Steps 1 through 5 for each video-enabled Avaya one-X Communicator endpoint you want to configure.

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

Use this procedure to configure Polycom VSX/HDX series video conferencing systems and V500 and V700 video calling systems.

Checklist

When setting up these systems, you will need to know the following information:

- maximum number of VSX/HDX, V500, and V700 systems on your network
- PIN for each VSX/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.
- whether 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
- the IP codec sets you want to use
- the IP network regions you want use

Configuration Procedures

To configure Polycom VSX/HDX series video conferencing systems and V500/V700 video calling systems, you must perform the following steps:

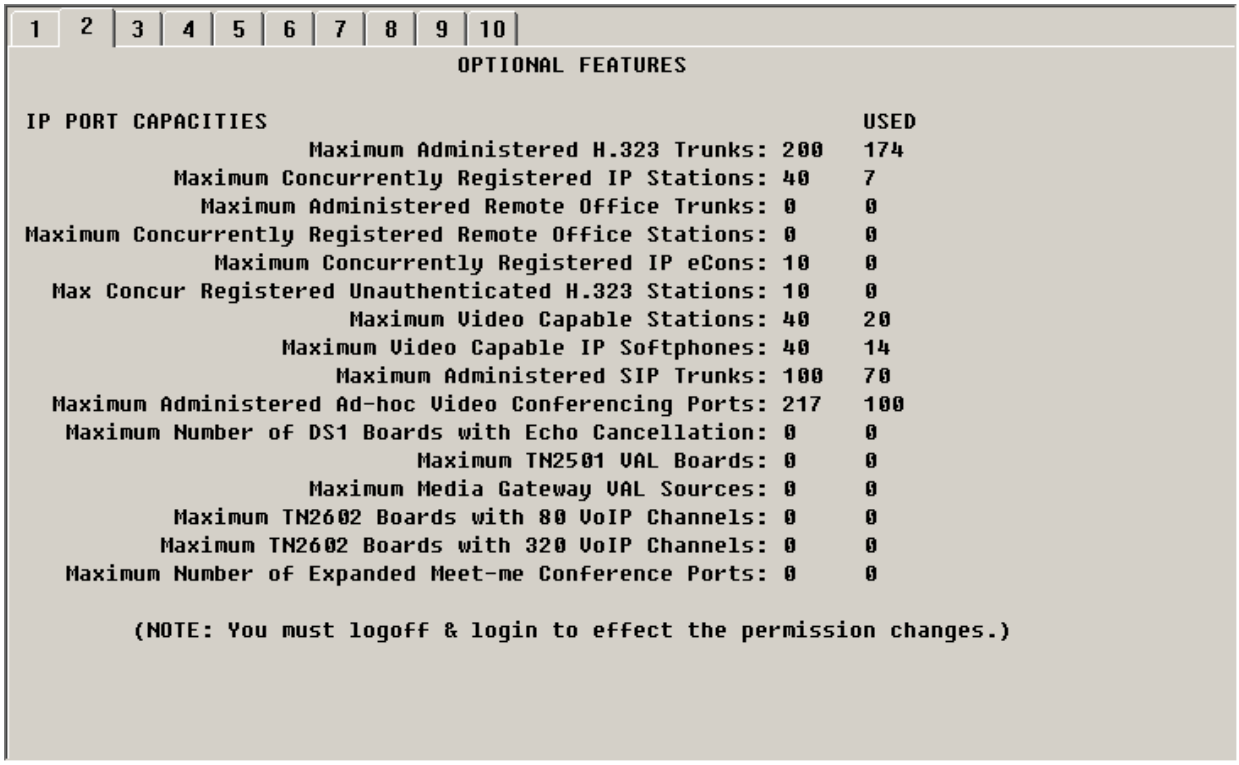
1. Determine the maximum number of video-capable H.323 stations your voice system supports. This step equates to checking the number of extensions in your license.
2. Configure the Class of Service if you want to use priority video calling.
3. Add a new station for the Polycom system.
4. Configure the Polycom system.
5. Optionally, configure the **Instant Transfer** button.

Procedure 1: Determine the Maximum Number of Video-Capable H.323 Stations Supported

To determine the maximum number of video-capable H.323 endpoints your voice system supports:

1. Use the **display system-parameters customer-options** command to access the Optional Features form.
2. On page 2 of the form, verify the **Maximum Video Capable Stations**. This number is provided by the RFA license file. The **Maximum Video Capable Stations** was determined using the following criteria:
   - Each V500/V700 system is considered to be **one** station.
   - Each single-point VSX system is considered to be **one** station.
   - Each VSX multipoint system can be **three** to **five** stations. Each system supports six sites in a call, but this includes the caller, so only five stations need to be administered.
   - Each HDX system can be three stations for "Multipoint Plus Four" (MP-4) and seven stations for "Multipoint Plus Eight" (MP-8) for the HDX9004. The basic rule is that for an N-way multipoint system, N-1 consecutive H.323 stations are required. So, for example, a HDX9004 with an MP-8 license requires seven H.323 stations with adjacent extensions, such as 71862 to 71868. The adjacent extensions and a circular **`hunt-to-station`** configuration ensure that the next available extension is accessed with multiple dial-ins.
   - The HDX9002 only has "Multipoint Plus Four"(MP-4) as an option.

Figure 8: Example of Page 2 of the Optional Features Form



```
1  2  3  4  5  6  7  8  9  10
                        OPTIONAL FEATURES

IP PORT CAPACITIES                                          USED
                    Maximum Administered H.323 Trunks: 200  174
          Maximum Concurrently Registered IP Stations: 40   7
            Maximum Administered Remote Office Trunks: 0    0
Maximum Concurrently Registered Remote Office Stations: 0   0
             Maximum Concurrently Registered IP eCons: 10   0
  Max Concur Registered Unauthenticated H.323 Stations: 10   0
                       Maximum Video Capable Stations: 40   20
                  Maximum Video Capable IP Softphones: 40   14
                      Maximum Administered SIP Trunks: 100  70
  Maximum Administered Ad-hoc Video Conferencing Ports: 217  100
   Maximum Number of DS1 Boards with Echo Cancellation: 0    0
                             Maximum TN2501 VAL Boards: 0    0
                    Maximum Media Gateway VAL Sources: 0    0
          Maximum TN2602 Boards with 80 VoIP Channels: 0    0
         Maximum TN2602 Boards with 320 VoIP Channels: 0    0
   Maximum Number of Expanded Meet-me Conference Ports: 0    0

       (NOTE: You must logoff & login to effect the permission changes.)
```

In this example, the system can have a maximum of 40 video-capable stations. Currently, 20 video-capable H.323 stations are being used.

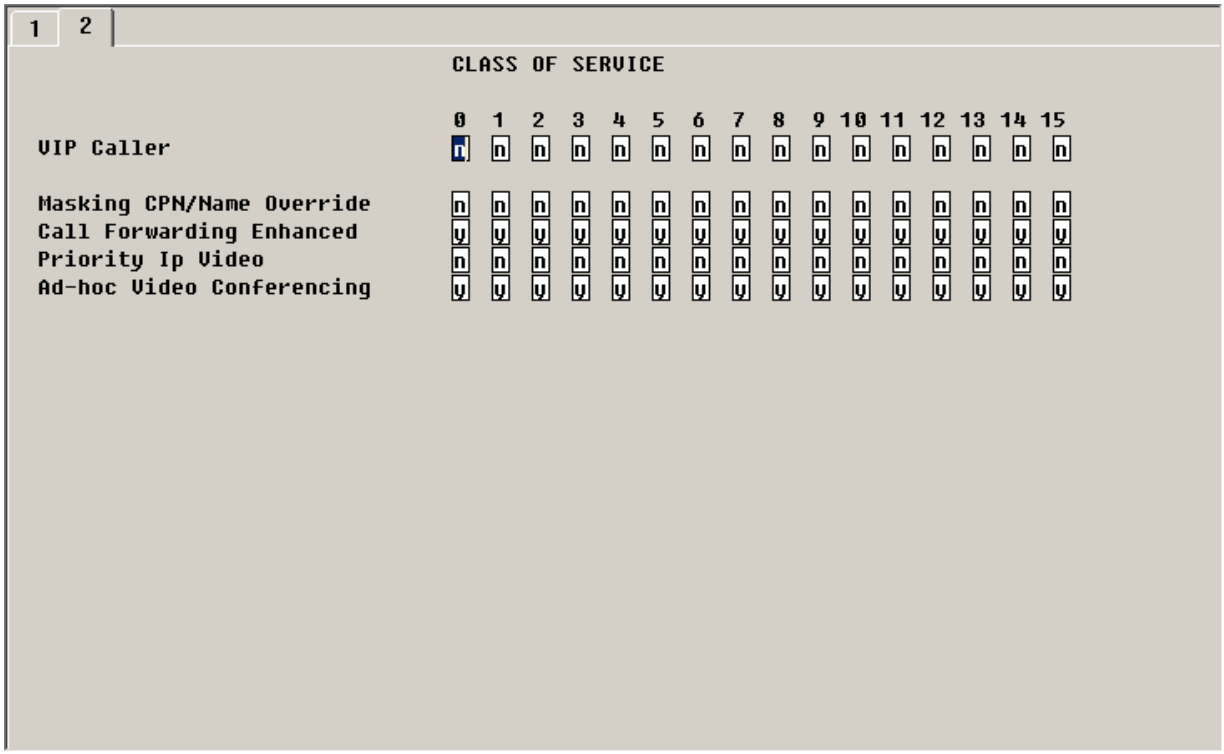
Procedure 2: Configure Class of Service

Perform this procedure if you want to allow priority video calling.

To configure the Class of Service:

1. Use the **change cos** command to access the Class of Service form.
2. Go to page 2 of the form.

Figure 9: Example of Page 2 of the Class of Service Form



3. Set **Priority Video Calling** for the appropriate COS levels.

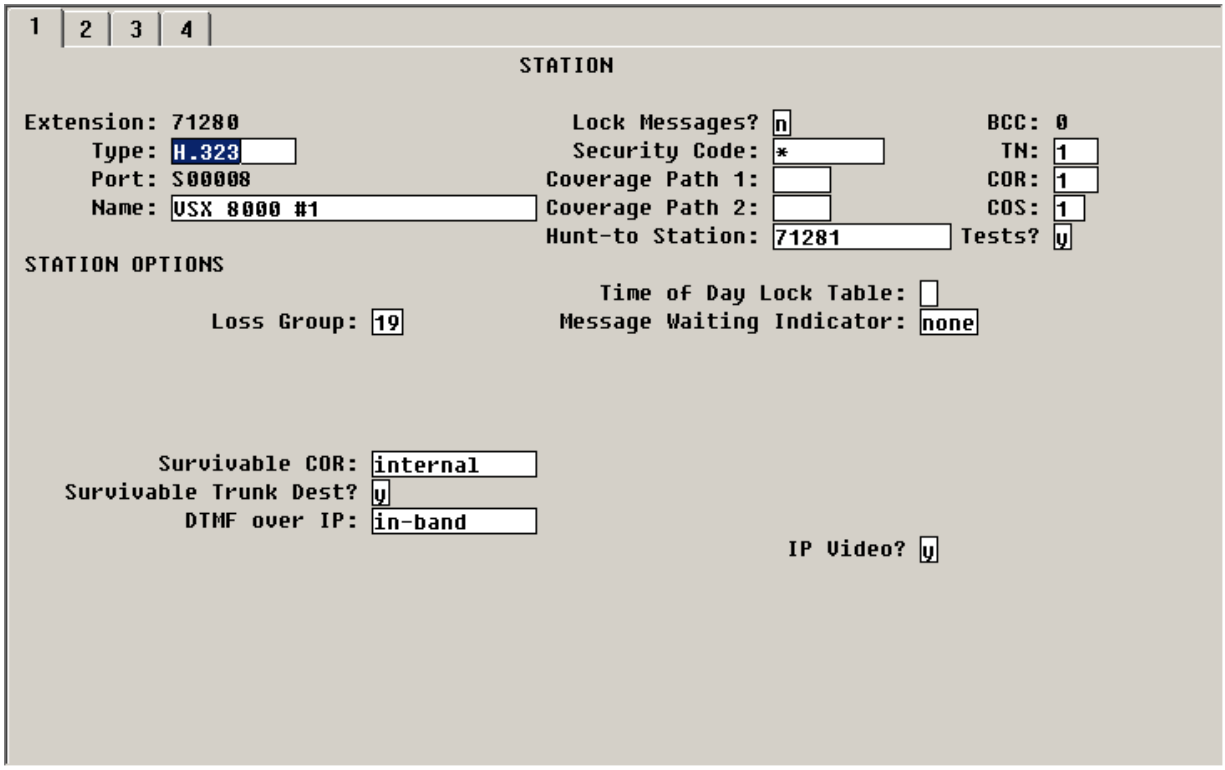
Procedure 3: Add a Station for the Polycom System

To add a station:

1. Use the **add station** command.

   The Station form appears.

Figure 10: Example of Page 1 of the Station Form



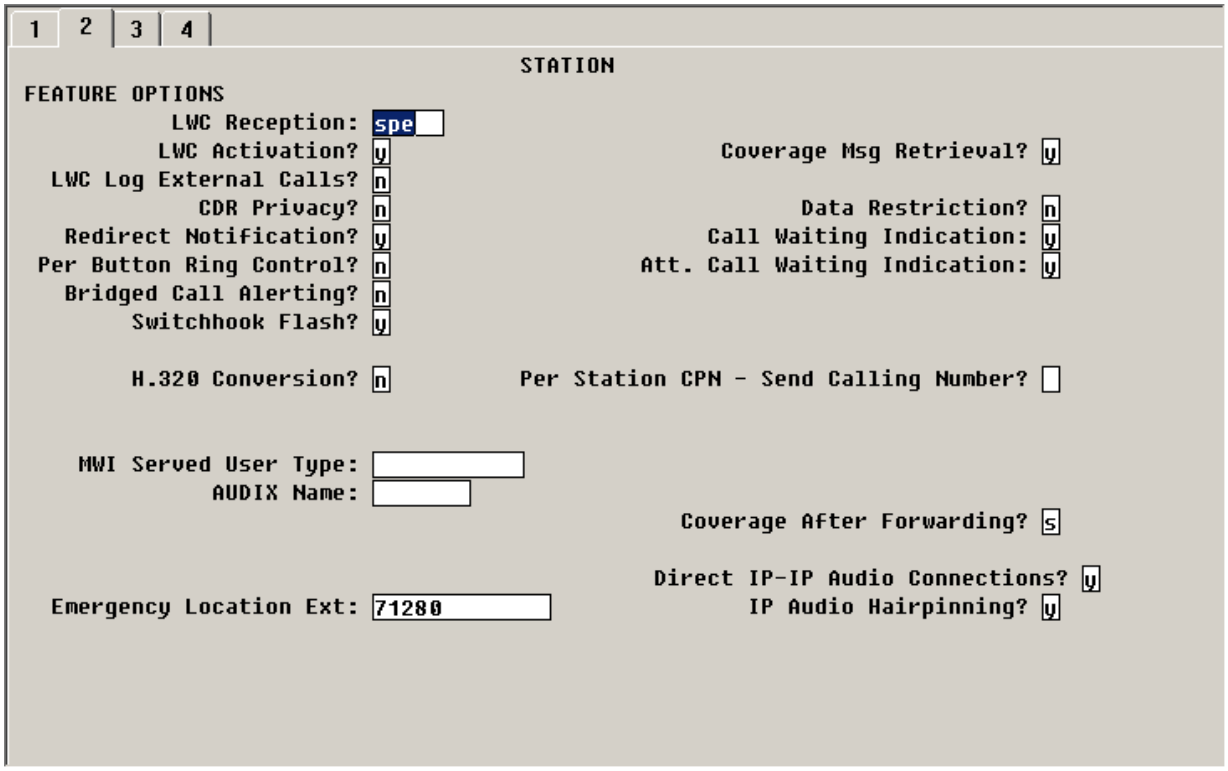
2. Enter the appropriate information for this station.
3. Set **Type** to **H.323**.
4. Set **Security Code** to the “pin” you will administer for the VSXHDX or V500 system.
5. Set **IP Video** to **y**.
6. If you want this station to be able to make priority video calls, make sure you select a COS level that has **Priority Video Calling** enabled. (See Procedure 2.)

   Note:

   You can create an alias for VSX/HDX stations.

7. Go to page 2 of the form.

Figure 11: Example of Page 2 of the Station Form



8. Set **Direct IP-IP Audio Connections** to **y**.
9. Set **IP Audio Hairpinning** to **y**.
10. 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 Procedure 4.)

11. If the VSX system has the multipoint option or IMCU option, perform the following steps:
    a. Use the **add station** command to add a second station for the Polycom system. The extension number should be one greater than the station added in the previous step 1.
    b. Set **Type** to **H.323**.
    c. Set **Security Code** to the “pin” you will administer for the VSX/HDX. Make sure the security code is the same as the previous station. Each station configured for the multipoint device must use the same security code.
    d. Set **IP Video** to **y**.
12. Repeat step 11 to create the third consecutive station.

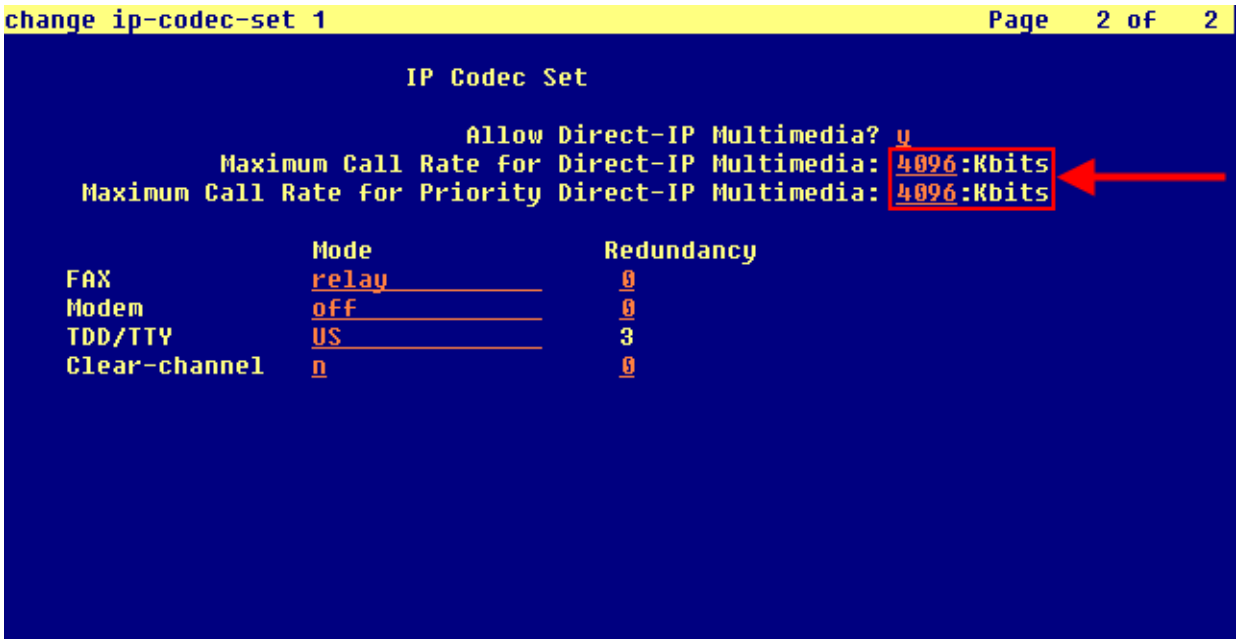
    Note:

    You can have up to seven stations.
13. Use the **change station *xx*** command (where ***xx*** is the first station you added for the Polycom system) to set **Hunt-to Station** to the second station you added for the Polycom system.
14. Use the **change station *xx*** command (where ***xx*** is the second station you added for the Polycom system) to set **Hunt-to Station** to the third station you added for the Polycom system.
15. Use the **change station *xx*** command (where ***xx*** is the third station you added for the Polycom system) to set **Hunt-to Station** to the first station you added for the Polycom system. All three stations must be in a circular hunt.

    Note:

    If you added more than three stations for the Polycom system, use the **change station *xx*** command to set **Hunt-to Station** for each station. All of the stations you add must be in a circular hunt.
16. Repeat Steps 1 through 15 to create the remaining consecutive stations as allowed by the Polycom MPPlus license.
17. Configure the call rate limit on the **IP Codec Set** form. You can access the IP Codec form by <information required>. You can set up the CM direct IP multimedia call rate limit to a maximum value of 4096 Kbits.

Figure 12: IP Codec Set Form



Procedure 4: Configure the Polycom System

To configure the Polycom system:

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. Select the **Enable IP H.323** check box.
5. Select 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 Procedure 4.
10. In the Number box in the Gateway area, enter the extension you specified.
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 **Diffserv** 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 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.

    Note:

    Remote control can have its RF band customized if controlling more than one system. Remote control can also be used to switch display modes by holding down the power button.

18. When finished, click the **Update** button.
19. Repeat Steps 1 through 18 for each Polycom system.

Procedure 5: Configure Instant Transfer

The **Instant Transfer** button enables Users to set up calls using the features on their desk telephone, rather than using the HDX dial pad. Users can also use this system to set up single calls as well as conferences and use features such as redial, auto-callback, and so on.

With **Instant Transfer**, Users can make or receive calls on their desk telephone and individually transfer each caller into their video room system to create a conference. For the successful operation of **Instant Transfer**, calls which originate on the 96xx must route over the internal IP video-enabled trunks. If calls route via PSTN, they are audio-only calls. It is important to note the video trunking feature interaction.

Note:

Transferring an existing conference to the room system will not allow the room system to host a proper video conference; It needs to receive the calls one at a time. Also, the room system is considered to be a member of the conference. The intent of **Instant Transfer** is for transfer to other stations only. Avaya does not recommend the **Instant Transfer** feature for MCU meeting rooms. Instead, Avaya recommends the “Ad-hoc 6-party video conferencing” feature.

To configure the **Instant Transfer** button:

- Use the **change station *xxxx,*** (where ***xxxx*** is the number of the station you want to modify) command to set **inst-trans Ext** to the location of the User's room system.

  The **inst-trans Ext** option is on the fourth screen. See Figure 13 for more information.

Figure 13: Inst-trans Button

```
change station XXXX                                  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: next
2: call-appr                                6: call-disp
3: call-appr                                7: send-calls Ext:
4: directory                                8: inst-trans Ext: YYYY
```

Note:

Avaya do not support this feature on SIP firmware versions of desksets.

Configure a Polycom RMX Series Video Conferencing Bridge Platform

This section describes how to configure a Polycom RMX series video conferencing bridge platform for use with an Avaya server.

Checklist

When setting up these systems, you will need to know the following information:

- the IP codec sets you want to use
- the IP network regions you want use
- the IP address of the IP board for the RMX system
- the IP address of the CLAN

Note:

Make sure you have the RMX Installation and Configuration guide available when you configure the RMX.

Configuration Procedures

To configure a Polycom RMX video conferencing bridge platform, you must perform the following steps:

1. Add an entry in the IP Node Names for the RMX system.
2. Add a two-way trunk group for the RMX system.
3. Add a signaling group for the RMX system.
4. Add members to the two-way trunk group for the RMX system.
5. Verify connectivity with the status signaling group command.
6. Create a route pattern for the trunk group.
7. Configure the dial plan so that the route pattern can be reached.
8. Configure the RMX system.
9. Make a test call.

Procedure 1: Add an Entry in the IP Node Names for the RMX System

To add an entry in the IP Node Names form for the RMX system:

1. Use the **change node-names ip** command to access the IP Node Names form.
2. In the Name field, enter a name for the RMX system.
3. In the corresponding IP Address field, enter the IP address of the signaling host for the RMX system.

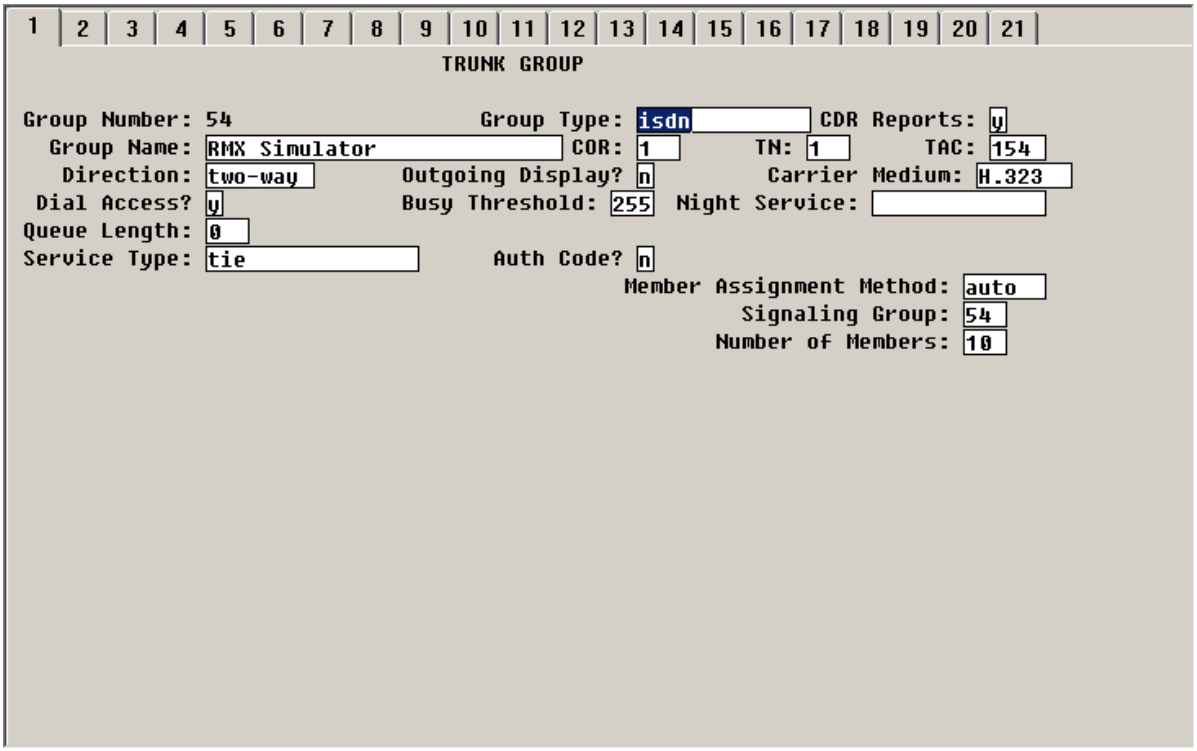
Procedure 2: Add a Two-Way Trunk Group for the RMX System

To add a two-way trunk group for the RMX system:

1. Use the **add trunk-group *xx*** command (where ***xx*** is the chosen trunk group) to access the Trunk Group form.

   The Trunk Group form appears.

Figure 14: Example of Page 1 of the Trunk Group Form



2. Set **Group Type** to **isdn**.
3. Set **Direction** to **two-way**.

4. Set **Carrier Medium** to **H.323**.
5. Set **Service Type** to **tie**.

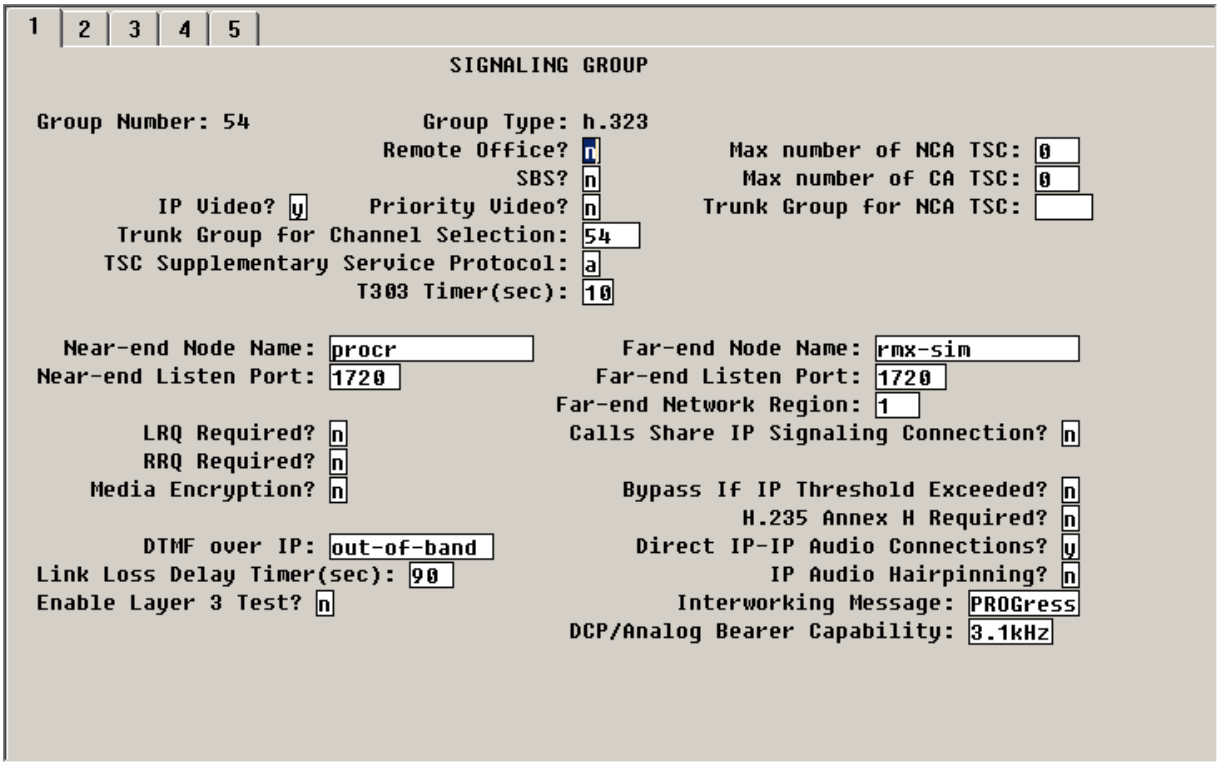
Procedure 3: Add a Signaling Group for the RMX System

To add a signaling group for the RMX system:

1. Use the **add signaling-group *xx*** command (where ***xx*** is the chosen signaling group) to access the Signaling Group form.

   The Signaling Group form appears.

Figure 15: Example of Page 1 of the Signaling Group Form



2. Set **Group Type** to **h.323**.
3. Set **IP Video** to **y**.
4. Set **Priority Video**. If you want all incoming calls to receive priority video transmissions, select **y**.
5. Set **Trunk Group for Channel Selection** to the two-way trunk group you added.
6. Set **Near-end Node Name**. For example, for an S8300 system, you would enter ***procr***. For an S8500 or S8700 system, you would enter the name of the CLAN board.

7. Set **Near-end Listen Port** to **1720**.
8. Set **LRQ Required** to **n**.
9. Set **RRQ Required** to **y**.
10. Set **ARQ Required** to **y**.
11. Set **Enable Layer 3 Test** to **n**.
12. Set **Far-end Node Name** to the name you entered for the RMX system.
13. Set **Far-end Listen Port** to **1720**.
14. Set the **Far-end Network Region**.
15. Set **Calls Share IP Signaling Connection** to **n**.
16. Set **Direct IP-IP Audio Connections** to **y**.
17. Set **IP Audio Hairpinning** to **n**.

Procedure 4: Add Members to the Two-Way Trunk Group

To add members to the two-way trunk group:

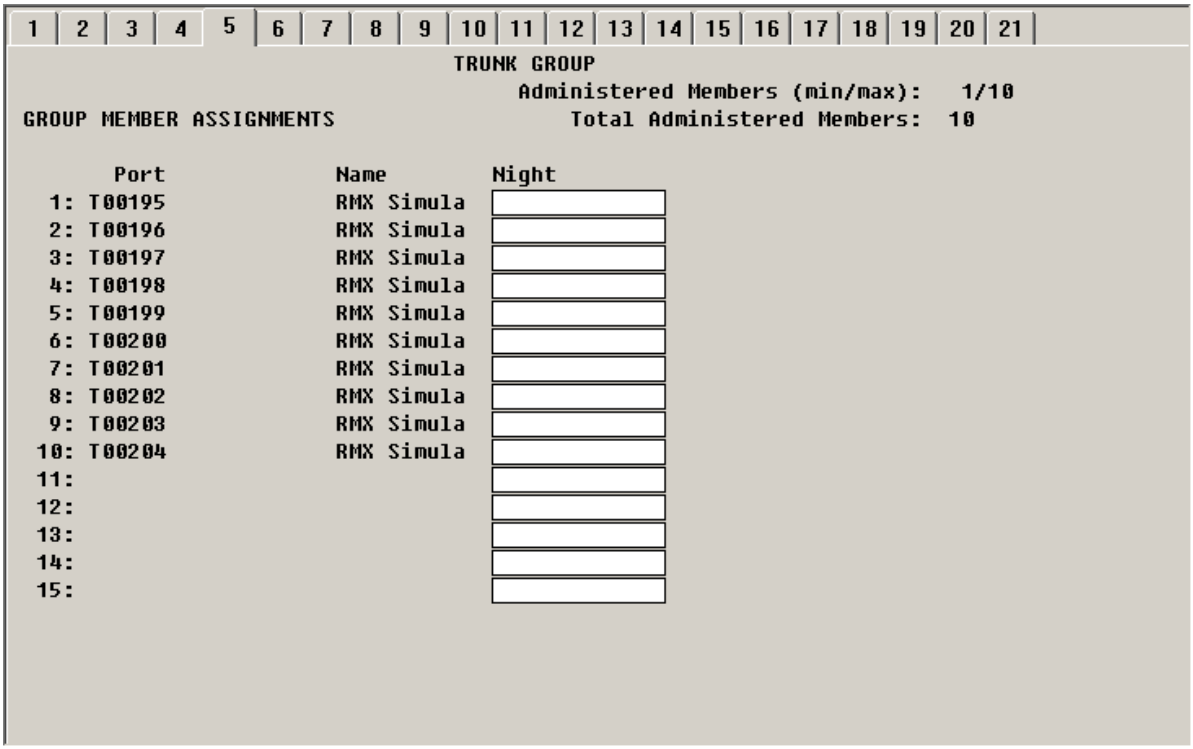
1. Use the **change trunk-group *xx*** command (where ***xx*** is the incoming trunk group you added) to access the Trunk Group form.

   The Trunk Group form appears.

2. Go to page 5 of the Trunk Group form.

   Page 5 of the Trunk Group form appears.

Figure 16: Example of Page 5 of the Trunk Group Form



3. Add members to the trunk group. The number of members depends on the maximum simultaneous calls an RMX supports.

Procedure 5: Create a Route Pattern for the RMX Trunk Group

To create a route pattern that points to the two-way trunk group:

1. Use the **change route-pattern *xx*** command (where ***xx*** is the route pattern you want to use) to access the Route Pattern form.

   The Route Pattern form appears.

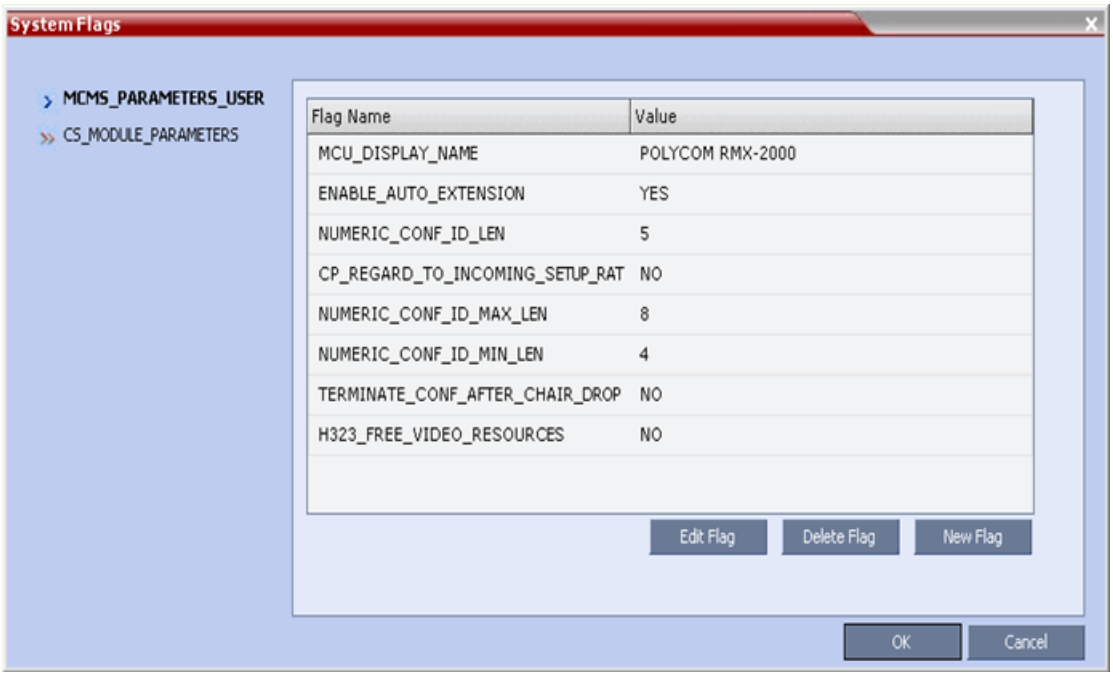
2. In the **Grp No** field, enter the number of the two-way trunk group you created for the RMX.

Procedure 6: Configure the RMX System

To configure the Polycom RMX system:

1. Install the RMX system and connect it to your network.
2. Upgrade the Polycom system software (if necessary).
3. Access the Polycom home page for the unit.
4. From the Setup menu, select the **System Parameters** tab.
5. Under 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

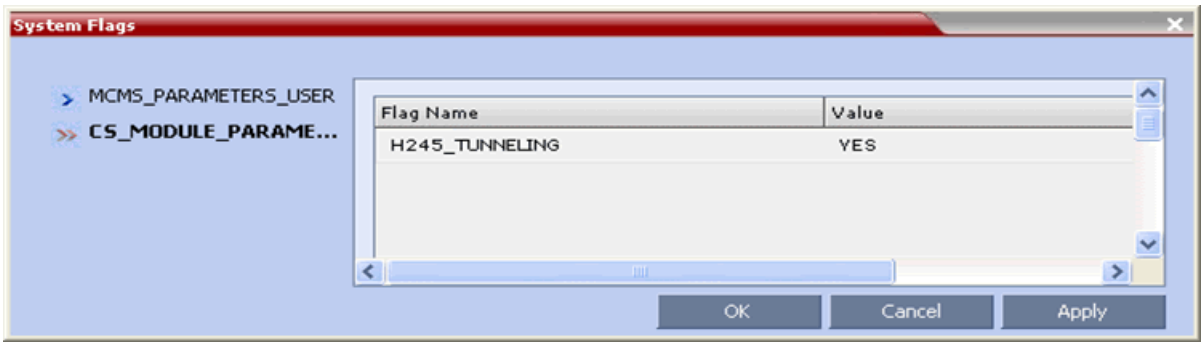
Figure 17: MCMS Parameters User Dialog



6. Under CS_MODULE_PARAMETERS, add the following information:

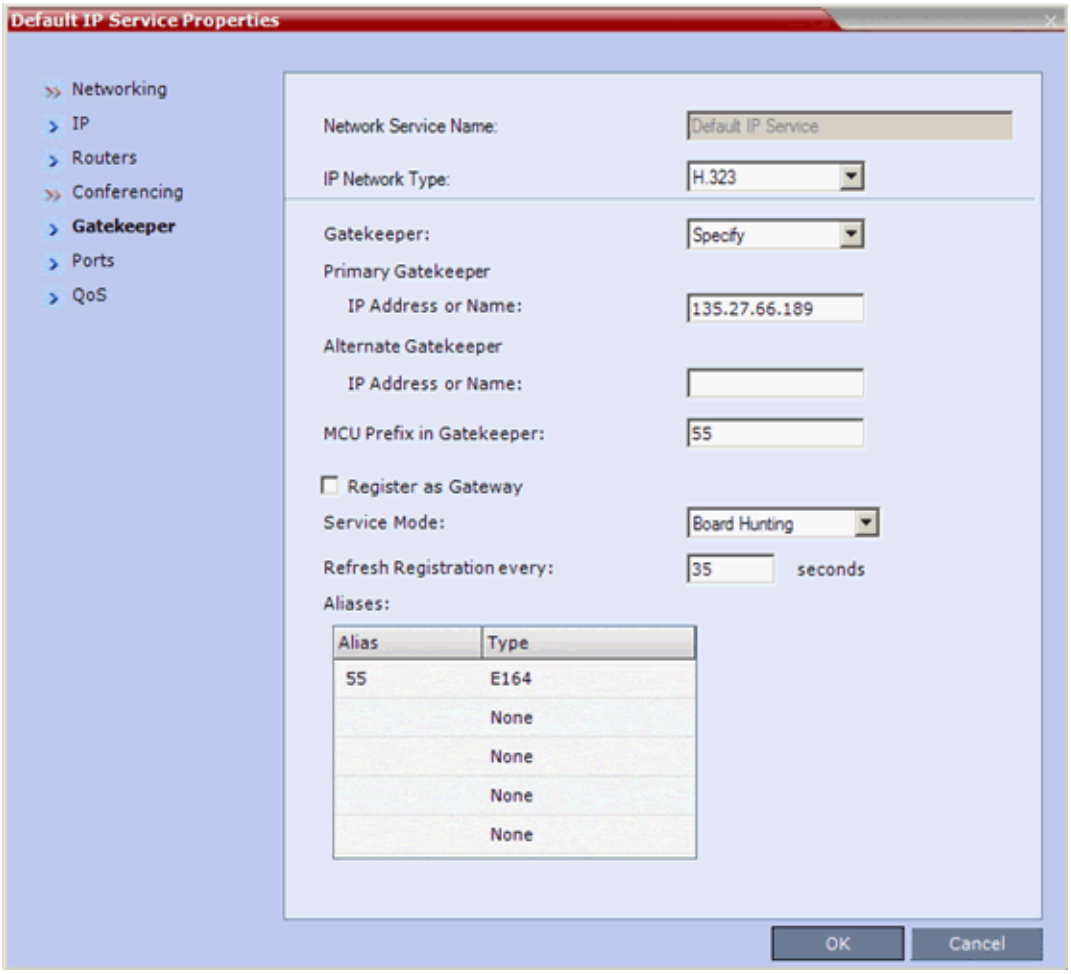
   H245_TUNNELING = YES

Figure 18: CS Module Parameters Dialog



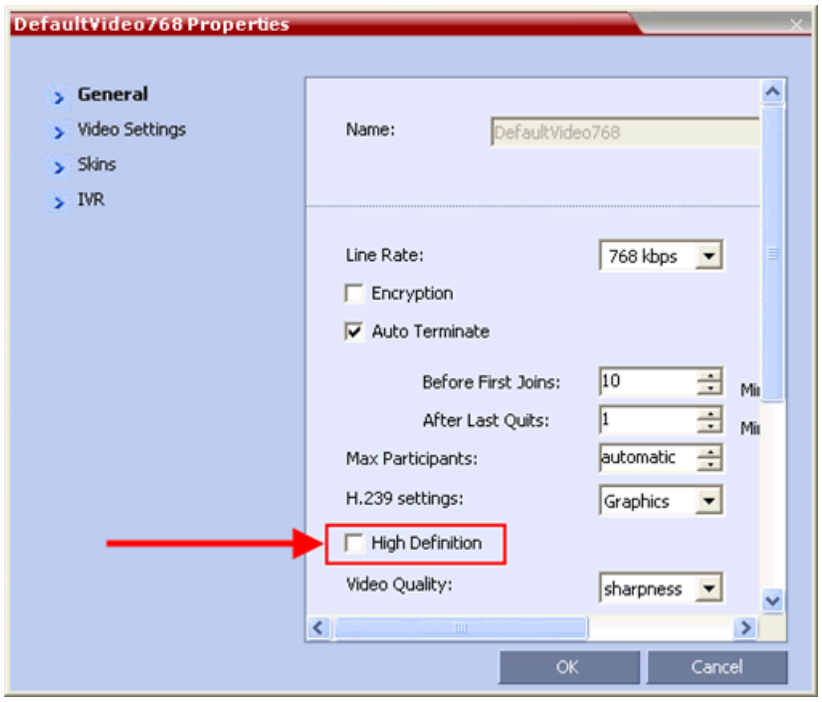
7. On the **Default IP Server Properties** dialog, create and configure a H.323 IP service with the Avaya Communication Manager settings, such as the CLAN IP address. Ensure that the MCU prefix and aliases match the dial plan that you configured on CM. Confirm via a status signaling group that the RMX has registered.

Figure 19: Default IP Service Properties Dialog



8. On the **Default Video Properties** dialog, configure the conference profile with the line rate, codec settings, and the high definition video switching option. Multiple meeting rooms can use this profile.

Figure 20: Default Video Properties Dialog



9. Create a meeting room to use a test direct dial conference ID.

If you want to configure Ad-hoc conferencing for the RMX system, go to Configure Ad-hoc Video Conferencing for a Polycom RMX Series Video Conferencing Bridge Platform on page 81.

Configure Ad-hoc Video Conferencing for a Polycom RMX Series Video Conferencing Bridge Platform

This section describes how to configure Ad-hoc video conferencing for a Polycom RMX series video conferencing bridge platform.

Checklist

When setting up Ad-hoc conferencing on a Polycom RMX system, you will need to know the following information:

- the IP codec sets you want to use
- the IP network regions you want use
- the IP address of the IP board for the RMX system
- the IP address of the CLAN

Note:

Make sure you have the RMX Installation and Configuration guide available when you configure the RMX.

Configuration Procedures

To configure Ad-hoc conferencing, you must perform the following steps:

1. Configure the RMX for use with an Avaya server.
2. Determine the maximum number of Ad-hoc video conferencing ports your voice system supports.
3. Configure the Class of Service for Ad-hoc video conferencing.
4. Configure the RMX system for Ad-hoc conferencing.
5. Configure a video bridge.

Procedure 1: Configure the Polycom RMX for Use with an Avaya Server

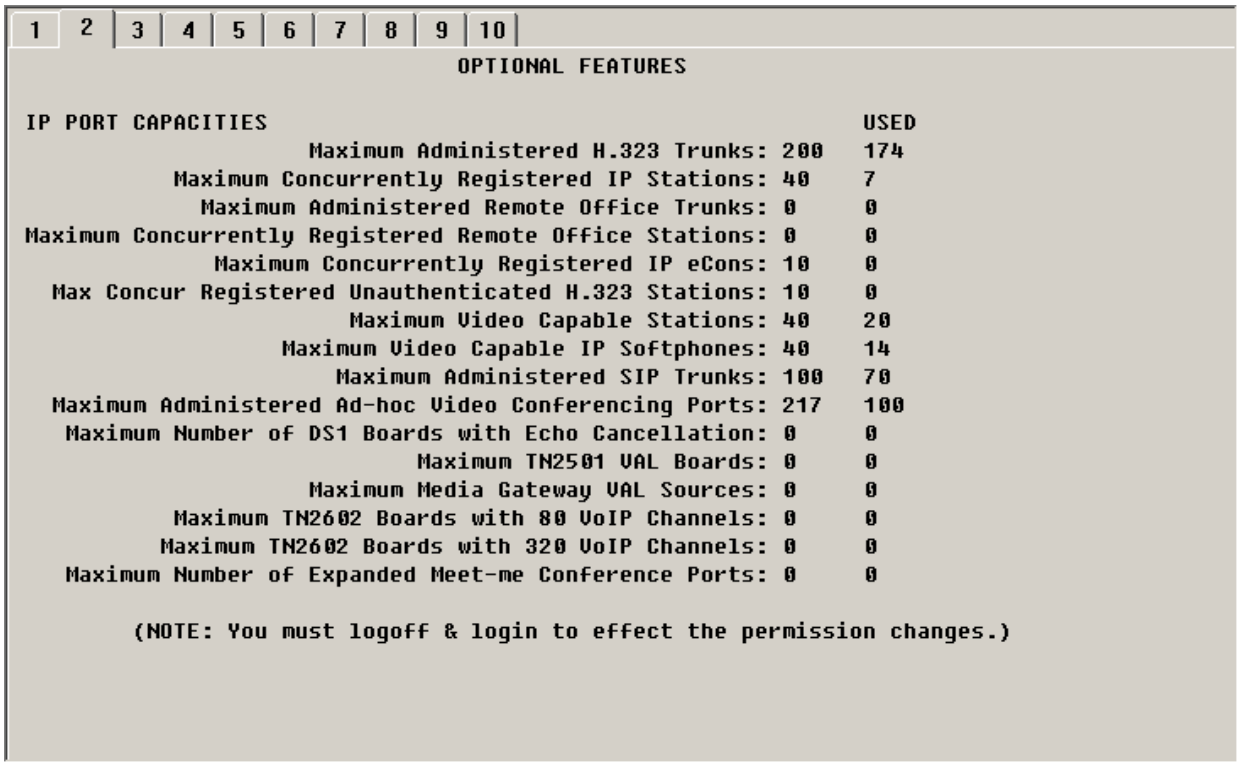
Perform the procedures in the section Configure a Polycom RMX Series Video Conferencing Bridge Platform on page 72 to configure the Polycom RMX system. After performing these procedures, go to Procedure 2: Determine the Maximum Number of Ad-hoc Video Conferencing Ports Supported on page 82.

Procedure 2: Determine the Maximum Number of Ad-hoc Video Conferencing Ports Supported

To determine the maximum number of Ad-hoc video conferencing ports your voice system supports:

1. Use the **display system-parameters customer-options** command to access the Optional Features form.
2. On page 2 of the form, verify **Maximum Administered Ad-hoc Video Conferencing Ports**. 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.

Figure 21: Example of Page 2 of the Optional Features Form



```
1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10

                          OPTIONAL FEATURES

IP PORT CAPACITIES                                              USED
                    Maximum Administered H.323 Trunks: 200      174
          Maximum Concurrently Registered IP Stations: 40       7
            Maximum Administered Remote Office Trunks: 0        0
Maximum Concurrently Registered Remote Office Stations: 0       0
             Maximum Concurrently Registered IP eCons: 10       0
  Max Concur Registered Unauthenticated H.323 Stations: 10      0
                      Maximum Video Capable Stations: 40        20
                  Maximum Video Capable IP Softphones: 40       14
                     Maximum Administered SIP Trunks: 100       70
  Maximum Administered Ad-hoc Video Conferencing Ports: 217     100
   Maximum Number of DS1 Boards with Echo Cancellation: 0       0
                            Maximum TN2501 VAL Boards: 0        0
                    Maximum Media Gateway VAL Sources: 0        0
          Maximum TN2602 Boards with 80 VoIP Channels: 0        0
         Maximum TN2602 Boards with 320 VoIP Channels: 0        0
   Maximum Number of Expanded Meet-me Conference Ports: 0       0

       (NOTE: You must logoff & login to effect the permission changes.)
```

In this example, the system can have a maximum of 217 administered Ad-hoc video conferencing ports. Currently, 100 Ad-hoc video conferencing ports are being used.

Procedure 3: Configure Class of Service

To configure the Class of Service:

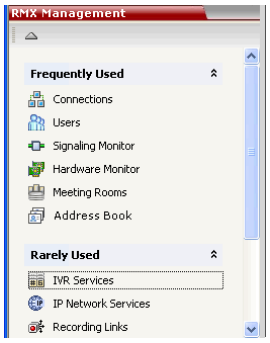
1. Use the **change cos** command to access the Class of Service form.
2. Go to page 2 of the form.
3. Set **Ad-hoc Video Conferencing** for the appropriate COS levels.

Procedure 4: Configure the RMX System

On the Polycom RMX system, perform the following steps for Ad-hoc conferencing:

1. Create a Conference IVR Service or configure an existing one:
   a. Navigate to **RMX Management** > **Rarely Used** > **IVR Services**, as shown in Figure 22.

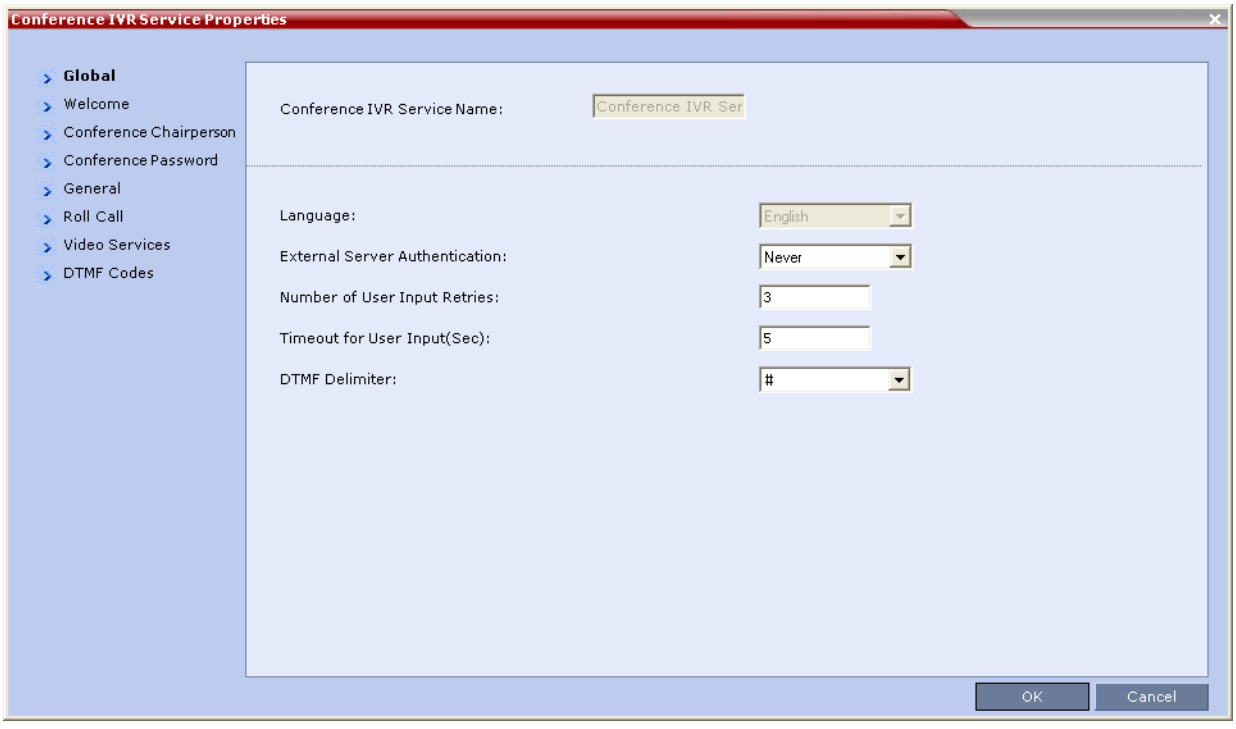
Figure 22: IVR Services



b. Edit the properties, as described below.

Figure 23 shows the **Properties** dialog.

Figure 23: IVR Properties



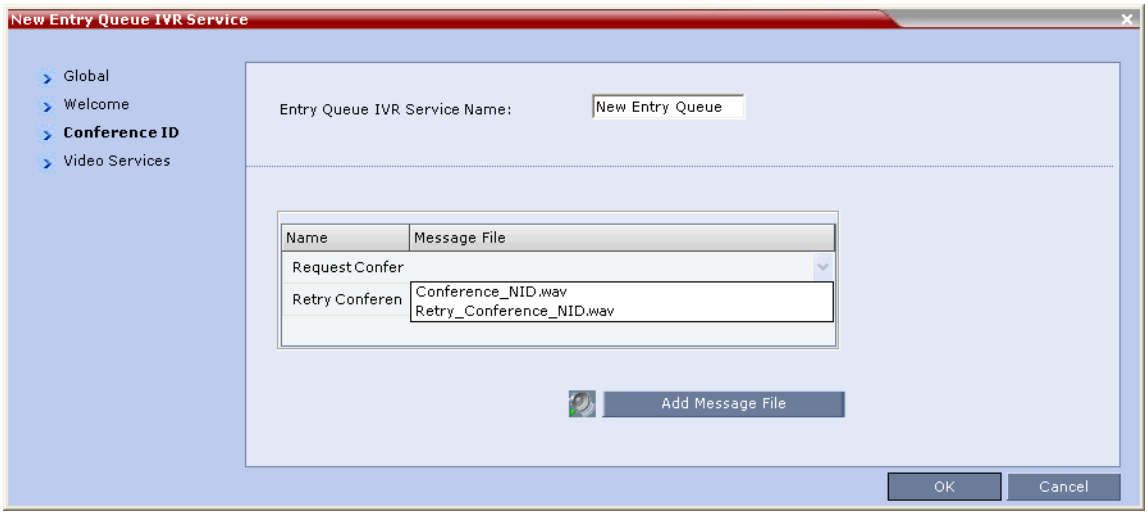
- On the **Welcome** tab, disable the **Enable Welcome Messages** check box.
- On the **Conference Chairperson** tab, disable the **Enable Chairperson Messages** check box.

- On the **Conference Password** tab, disable the **Enable Password Messages** check box.
- On the **General** tab, deselect any .wav file for the First to Join announcement.
- On the **Roll Call** tab, disable the **Enable Roll Call** check box.
- On the **Video Services** tab, disable the **Click&View** checkbox.

2. Create an Entry Queue IVR Service or configure an existing one.

   You can accept the default settings for all properties. However, you must manually select the audio files on the **Conference ID** tab, as shown in Figure 24.

Figure 24: Conference ID Tab



3. Set a silence .wav file as the IVR message. A silence .wav file disables music from being played to the first party who joins the conference.

   If you have already created a silence .wav file, begin with step h.

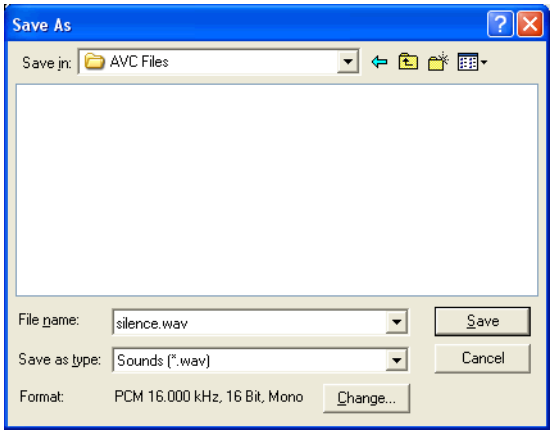
   If you do not have a silence .wav file, begin with step a.

   a. Open the **Windows Sound Recorder** application from **Start** > **Programs** > **Accessories** > **Entertainment** > **Sound Recorder**, as shown in Figure 25.

Figure 25: Windows Sound Recorder

b. From the **File** menu, select **Save As...** to display the **Save As** dialog, as shown in Figure 26.

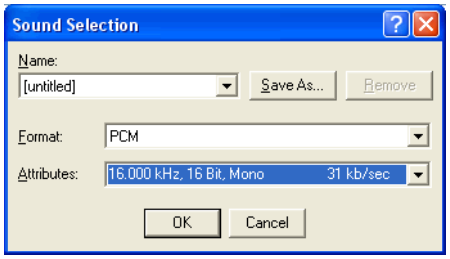
Figure 26: Save As Dialog



c. In the **File Name** field, enter `silence.wav`.

d. Click the **Change** button to display the **Sound Selection** dialog, as shown in Figure 27.

Figure 27: Sound Selection Dialog



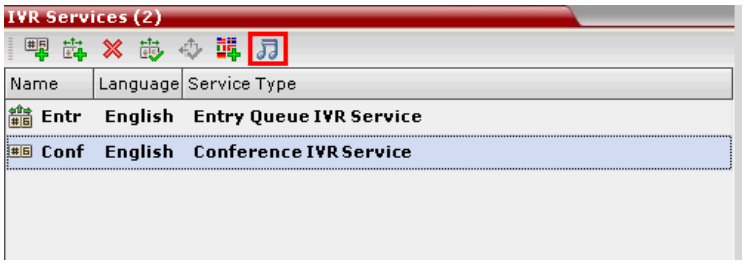
e. From the **Format** drop-down list, select **PCM**.

f. From the **Attributes** drop-down list, select **16.000 kHz, 16 Bit, Mono**.

g. Click **OK** on the **Sound Selection** dialog and then click **Save** on the **Save As** dialog.

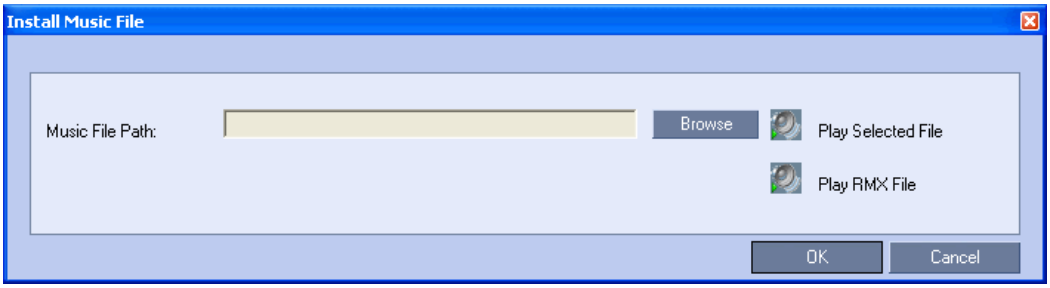
h. Under the **IVR Services** tab, click the **Music** icon to display the **Install Music File** dialog. Figure 28 shows the **Music** icon.

Figure 28: Music Icon



i. Set the silence.wav file as the IVR message. Figure 29 shows the **Install Music File** dialog.

Figure 29: Install Music File Dialog

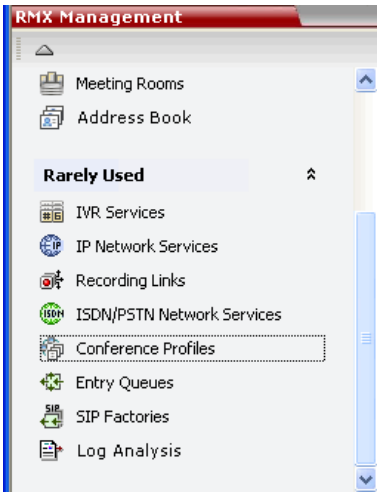


j. Click **OK**.

4. Create conference profiles for Ad Hoc (and Meeting Room, if desired) style conferences. You should create one profile for standard users and another profile for priority users.

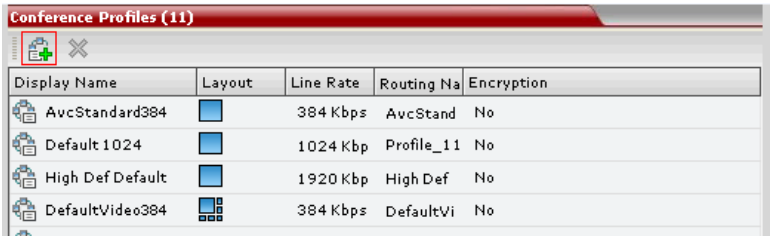
   a. Navigate to **RMX Management** > **Rarely Used** > **Conference Profiles**, as shown in Figure 30.

Figure 30: Conference Profiles



b. Click the **New Profile** icon to display the **New Profile** dialog. Figure 31 shows the **New Profile** icon.

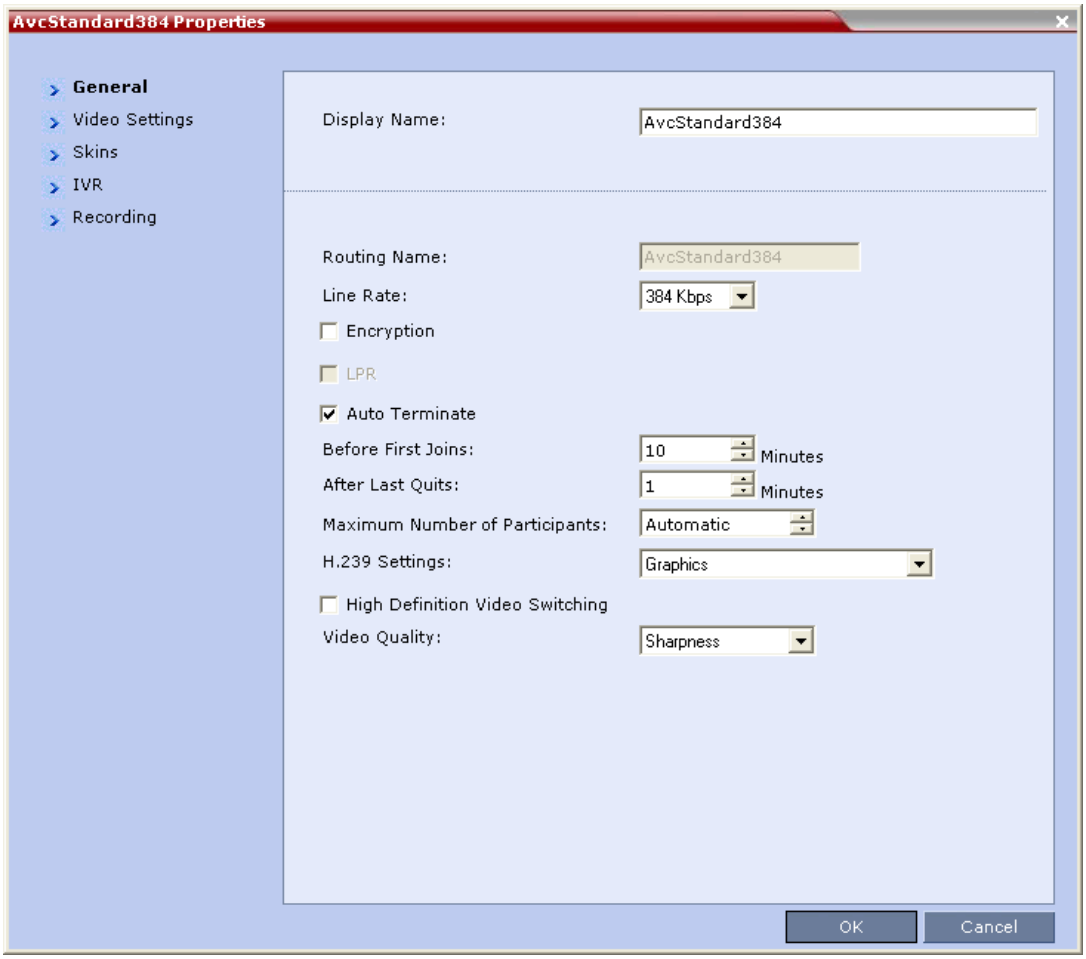
Figure 31: New Profile Icon



c. Configure the properties, as described below.

Figure 32 shows the **Properties** dialog.

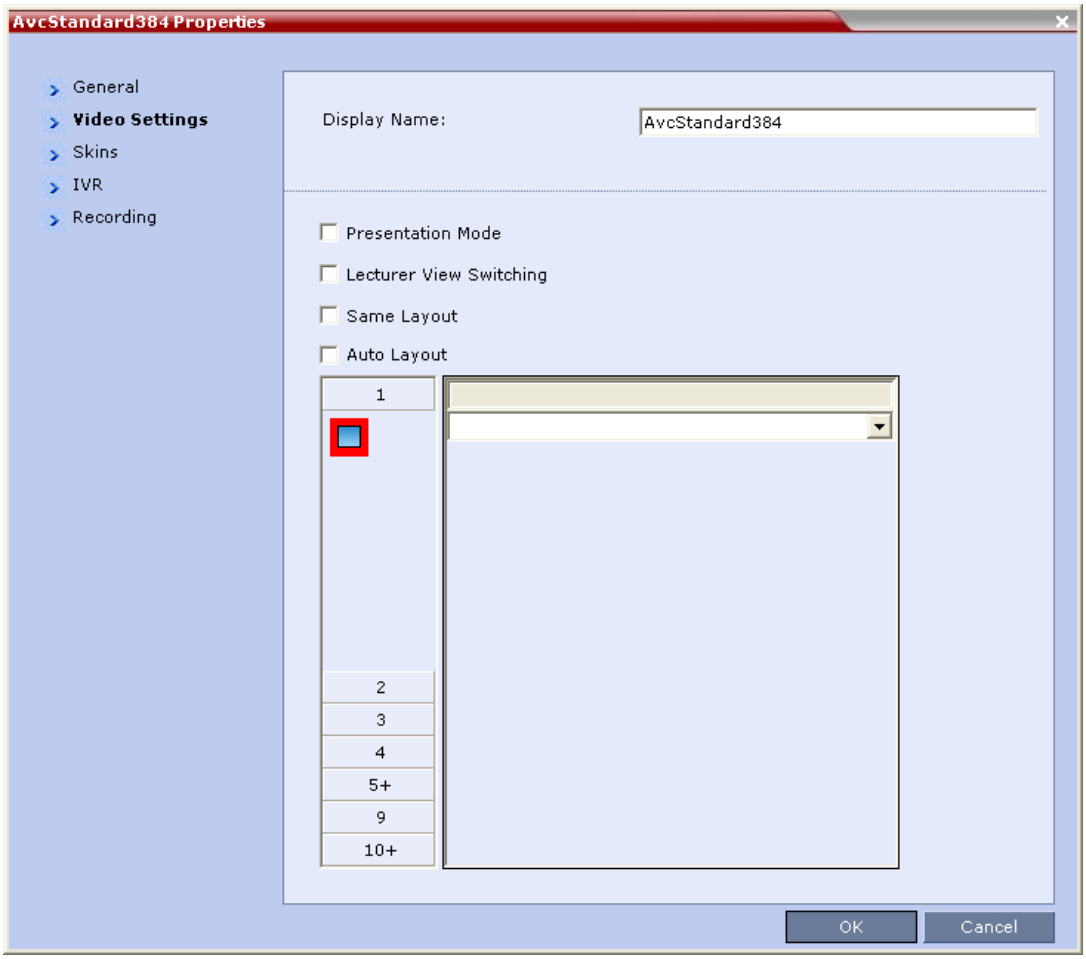
Figure 32: Conference Profile Properties



- On the **General** tab, select your desired line rate from the **Line Rate** drop-down list. This is the primary difference between standard and priority conferences.
  - Enable the **Auto Terminate** check box.
  - Set the **Maximum Number of Participants** to **Automatic**.
- On the **Video Settings** tab, ensure that **Auto Layout** is not enabled.
  - On the Layout control, select 1. This layout displays the active speaker only and avoids the "hall of mirrors" effect when cascading. Figure 33 shows the **Video Settings** tab.

    These are the default values for Auto Layout and the Layout control.

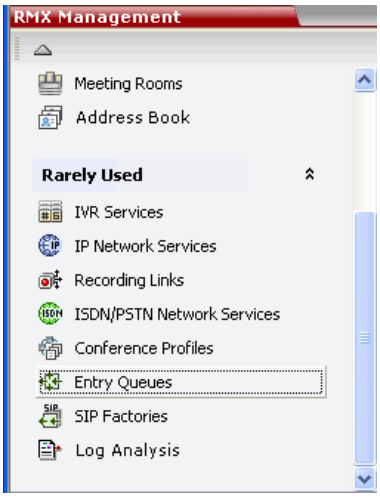
Figure 33: Video Settings Tab



- On the **IVR** tab, from the **Conference IVR Service** drop-down list, select the IVR service that you created in step 1.

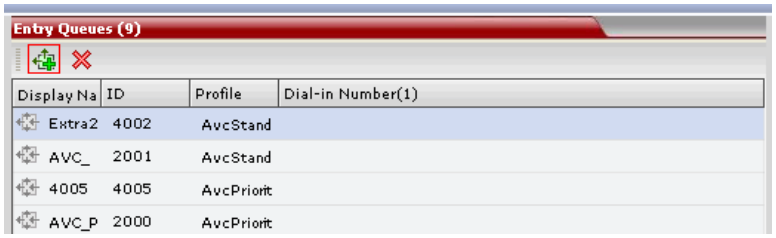
5. Create two entry queues, one for standard conferences and one for priority conferences.
   a. Navigate to **RMX Management** > **Rarely Used** > **Entry Queues**, as shown in Figure 34.

Figure 34: Entry Queues



b. Click the **New Entry Queue** icon to display the **New Entry Queue** dialog. Figure 35 shows the **New Entry Queue** icon.

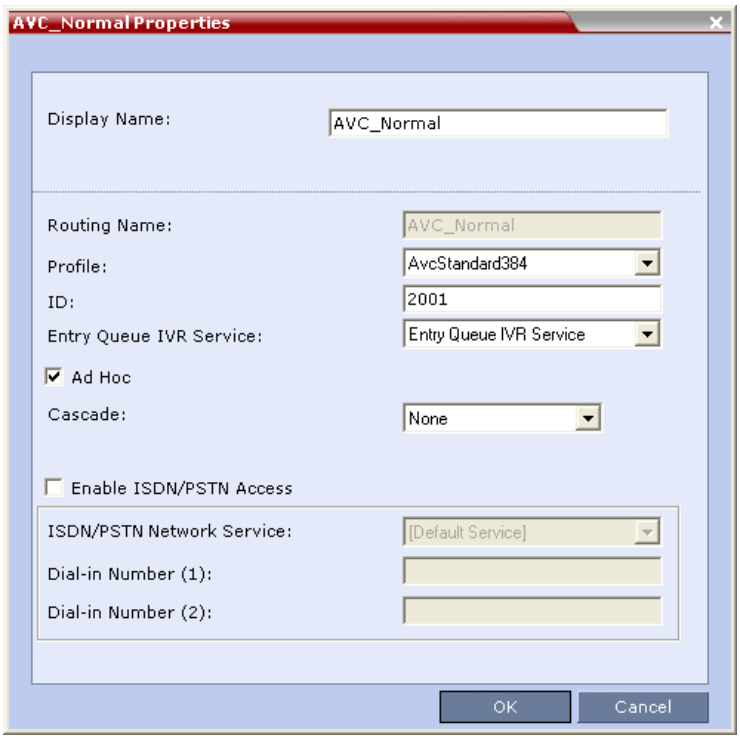
Figure 35: New Entry Queue Icon



c. Configure the properties, as described below.

Figure 36 shows the **New Entry Queue/Properties** dialog.

Figure 36: New Entry Queue/Properties Dialog



- From the **Profile** drop-down list, select one of the conference profiles that you created in step 4.
- From the **Entry Queue IVR Service** drop-down list, select the Entry Queue IVR Service that you created in step 2.
- In the **ID** field, enter an ID. Avaya Communication Manager will later refer to this ID as the factory number.
- Enable the **Ad Hoc** check box.

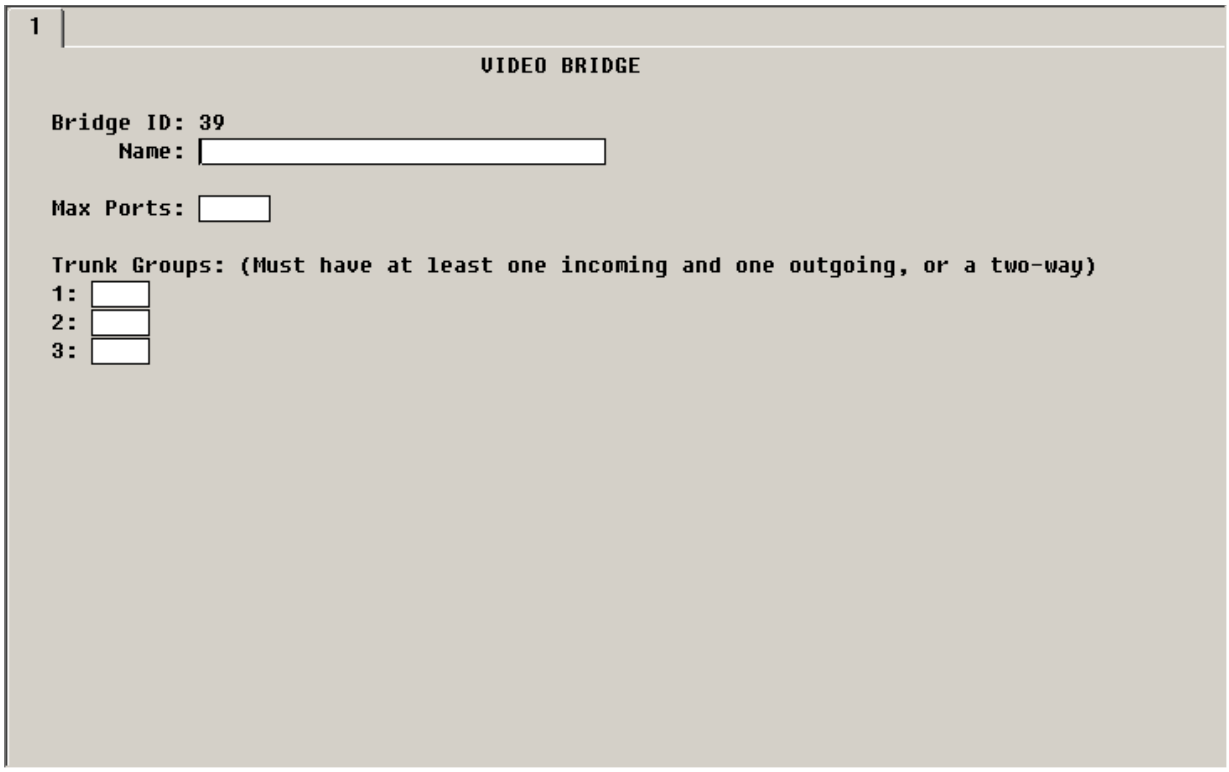
d. Click **OK**.

Procedure 5: Configure a Video Bridge

To configure a video bridge:

1. Use the **add video-bridge *xx*** command (where ***xx*** is the bridge number between 1 to 40) to access the Video Bridge form.

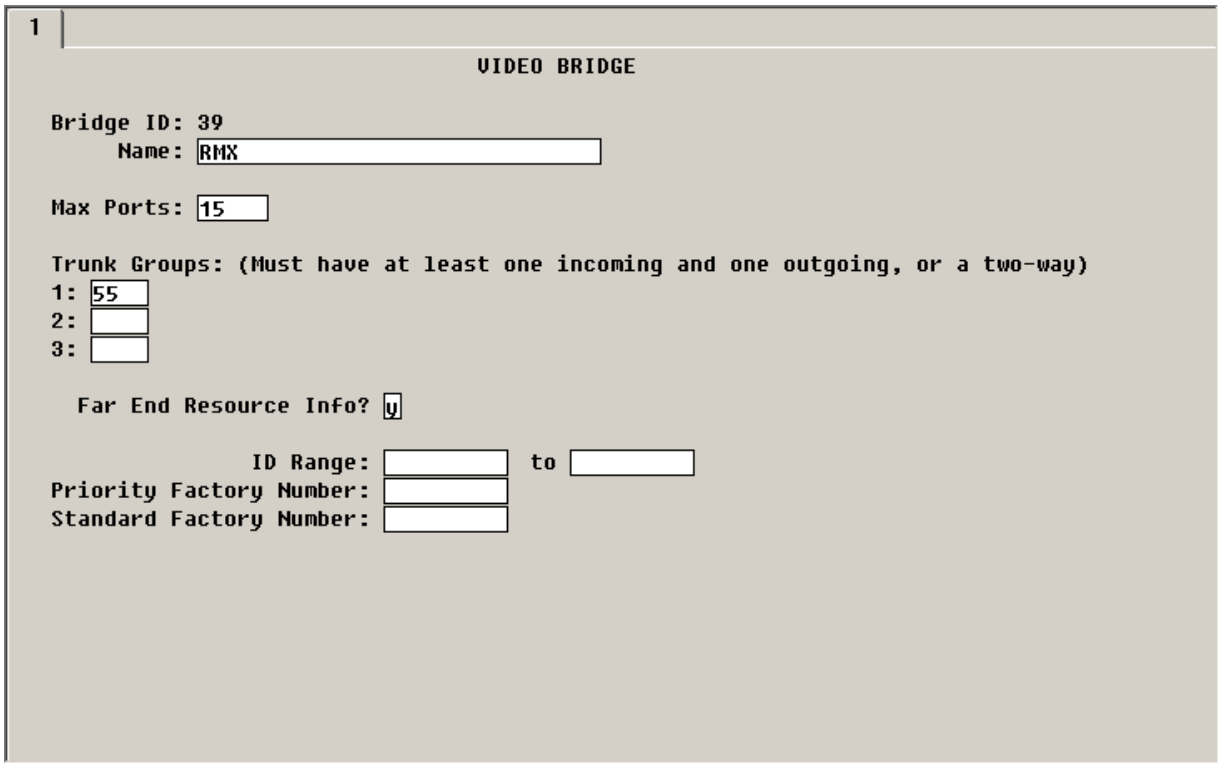
Figure 37: Example of the Video Bridge Form



2. In **Name**, enter the name for this video bridge (for example, *Ad Hoc Video Bridge - RMX*).
3. Set **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.
4. In **Trunk Groups**, enter the administered two-way ISDN H.323 trunk groups you added in Procedure 2: Add a Two-Way Trunk Group for the RMX System on page 73. All entries must be of the same carrier type (that is, all H.323 trunks).

   The Far End Resource Info, ID Range, Priority Factory Number, and Standard Factory Number fields appear.

Figure 38: Example of the Video Bridge Form



5. Make sure **Far End Resource Info?** is set to **y**.
6. Set **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 Automatic Alternate Routing (AAR) and Unified Dial Plan (UDP) are not used to connect to these meeting room numbers. Conference IDs (and factory numbers) are completely independent of the dial plan. As a result, you can set up several video bridges with exactly the same conference IDs and numbers. (This will make it easier for you to maintain configurations and swap hardware.)
7. Set **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).

8. Set **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. You cannot leave both fields blank.

Display Capacity for Ad-hoc Video Conferencing

To display the 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.)

View Video Conferencing Bridges

Use the **list video-bridge** command to view the video conferencing bridges administered on your system.

Configure a Polycom MGC-25 Video Conferencing Bridge Platform for an Avaya S8300 Server

This section describes how to configure a Polycom MGC-25 video conferencing bridge platform for use with an Avaya S8300 server.

Checklist

When setting up these systems, you will need to know the following information:

- the IP codec sets you want to use
- the IP network regions you want use
- the IP address of the IP board for the MGC system
- the IP address of the CLAN

Configuration Procedures

To configure a Polycom MGC-25 video conferencing bridge platform for use with an Avaya S8300 server, you must perform the following steps:

1. Add an entry in the IP Node Names for the MGC system.
2. Add a two-way trunk group for the MGC system.
3. Add a signaling group for the MGC system.
4. Add members to the two-way trunk group for the MGC system.
5. Create a route pattern for the trunk group.
6. Configure the MGC system.

Procedure 1: Add an Entry in the IP Node Names for the MGC System

To add an entry in the IP Node Names form for the MGC system:

1. Use the **change node-names ip** command to access the IP Node Names form.
2. In the **Name** field, enter a name for the MGC system.
3. In the corresponding **IP Address** field, enter the IP address of the IP board for the MGC system.

Procedure 2: Add a Two-Way Trunk Group for the MGC System

To add a two-way trunk group for the MGC system:

1. Use the **add trunk-group *xx*** command (where ***xx*** is the chosen trunk group) to access the Trunk Group form.

   The Trunk Group form appears.

2. Set **Group Type** to **isdn**.
3. Set **Direction** to **two-way**.
4. Set **Carrier Medium** to **H.323**.
5. Set **Service Type** to **tie**.

Procedure 3: Add a Signaling Group for the MGC System

To add a signaling group for the MGC system:

1. Use the **add signaling-group *xx*** command (where ***xx*** is the chosen signaling group) to access the Signaling Group form.

   The Signaling Group form appears.

2. Set **Group Type** to **h.323**.
3. Set **IP Video** to **y**.
4. Set **Priority Video**. If you want all incoming calls to receive priority video transmissions, select **y**.
5. Set **Trunk Group for Channel Selection** to the two-way trunk group you added.
6. Set **Near-end Node Name**. For example, for an S8300 system, you would enter ***procr***. For an S8500 or S8700 system, you would enter the name of the CLAN board.
7. Set **Near-end Listen Port** to **1720**.
8. Set **LRQ Required** to **n**.
9. Set **RRQ Required** to **y**.
10. Set **Enable Layer 3 Test** to **n**.
11. Set **Far-end Node Name** to the name you entered for the MGC system.
12. Set **Far-end Listen Port** to **1720**.
13. Set the **Far-end Network Region**.
14. Set **Calls Share IP Signaling Connection** to **n**.
15. Set **Direct IP-IP Audio Connections** to **y**.
16. Set **IP Audio Hairpinning** to **n**.

Procedure 4: Add Members to the Two-Way Trunk Group

To add members to the two-way trunk group:

1. Use the **change trunk-group *xx*** command (where ***xx*** is the incoming trunk group you added) to access the Trunk Group form.

   The Trunk Group form appears.

2. Go to page 5 of the Trunk Group form.

   Page 5 of the Trunk Group form appears.

3. Add members to the trunk group.

Procedure 5: Create a Route Pattern for the MGC Trunk Group

To create a route pattern that points to the two-way trunk group:

1. Use the **change route-pattern *xx*** command (where ***xx*** is the route pattern you want to use) to access the Route Pattern form.

   The Route Pattern form appears.

2. In the **Grp No** field, enter the number of the two-way trunk group you created for the MGC.

Procedure 6: Configure the MGC System

To configure the Polycom MGC system:

1. Install the MGC system and connect it to your network.
2. Upgrade the Polycom system software (if necessary).
3. Access the Polycom home page for the unit, and select **MCU Configuration>Network Services>IP>IP Default>Network Service Properties**.
4. Create a new H.323 service.
5. On the Settings tab, perform the following steps:
   a. Set **Protocol** to **H323**.
   b. Specify the **Subnet Mask**.
   c. Specify the **Default Router**.
6. On the DNS Settings tab, specify the appropriate DNS servers in the **Use DNS Servers** box.
7. On the H323 tab, perform the following steps:
   a. Make sure the **Forwarding** check box is not enabled.
   b. In the **Use Gatekeeper** box, specify the gatekeeper.
   c. In the **Preferred Gatekeeper IP Address** box, enter the CLAN IP address.

d. In the **Service Mode** box, enter **Pseudo Gatekeeper AVF**.

Note:

If **Pseudo Gatekeeper AVF** does not appear, you do not have the latest software. You must install the Avaya-enabled Polycom MGC Manager software.

e. In the Prefix box, enter the first digit of the extension numbers range in which the MCU resides.

f. Select the **Refresh H.323 Registrations** check box, and select a rate that is less than 60 seconds. (35 seconds is recommended.)

8. On the Spans tab, add a new IP Span.

a. In the **Circuit ID** box, enter a unique identifier for this new circuit.

b. In the **IP Address** box, enter the IP address of the IP card that will use H.323 signaling.

c. In the **H323 Alias 1** box, enter an H.323 ID of an alias for the board that Avaya Communication Manager will route calls to this MGC.

9. Define the IP1 configuration. In the **Circuit ID** box on the IP-Network Parameters tab, enter the unique identifier you specified in Step 6.

10. Create a meeting room in **Meeting Rooms and Entry Queues**. In the **Numeric ID** box on the General tab, enter the dialed digits excluding the prefix defined in the Network Service.

If you want to configure Ad-hoc video conferencing for the MGC system, go to Configure Ad-hoc Video Conferencing for a Polycom MGC Video Conferencing Bridge Platform on page 107.

Configure Polycom MGC Video Conferencing Bridge Platforms with Avaya S8500 and S87xx Server

This section provides a set of guidelines to configure Polycom MGC video conferencing bridge platforms for use with Avaya S8500 servers and Avaya S87xx servers. You must understand these guidelines before you administer these systems.

If you want to configure Ad-hoc conferencing for the MGC system (after you administer the MGC system for use with the Avaya server), go to Configure Ad-hoc Video Conferencing for a Polycom MGC Video Conferencing Bridge Platform on page 107.

Trunk Groups

For incoming trunk groups, you must:

- Create one incoming trunk group per Polycom MGC system.
- Set the following parameters:
  - **Direction** to **incoming**.
  - **Service Type** to **tie**.
  - **Disconnect Supervision - In? t**o **y** to allow Polycom MGC-Avaya Communication Manager-Polycom MGC calls (that is, trunks calling trunks).

For outgoing trunk groups, you must:

- Create one “primary” outgoing trunk group for the “primary” Polycom MGC board (IP1).
- Set the following parameters:
  - **Direction** to **outgoing**.
  - **Service Type** to **tie**.
  - You may set **Outgoing Display** to **y**.
  - **Send Calling Number** to **y**. This allows participant matching in the Polycom MGC.
  - **Format** to **private**.
- If you want board redundancy, create one “secondary” outgoing trunk group for the other boards (IP2.n) in the Polycom MGC system.

Signaling Groups

For incoming signaling groups, you must:

- Create one incoming signaling group (RRQ signaling group) per MGC board in the Polycom MGC system for a primary CLAN. This incoming signaling group allows a Polycom MGC board to register and is used for incoming calls. The “primary” CLAN is the CLAN you want to use with the MGC. The IP address of this CLAN is administered on the MGC via the Polycom MGC Manager software.

  Keep in mind the following information:

  - For Avaya Communication Manager Release 3.0.1, one signaling group can support a maximum of 31 calls.
  - For Avaya Communication Manager Release 3.1 or later, one signaling group can support a maximum of 255 calls.

- Set the following parameters for the incoming signaling groups:
  - **IP Video?** to **y**.
  - **Priority Video.** If you want all incoming calls to receive priority video transmissions, select **y**.
  - **Trunk Group for Channel Selection**.
  - **Near-end Listen Port** to **1720**.
  - **Far-end Listen Port** to **1720**.
  - **ARQ Required?** to **y**.
  - **RRQ Required?** to **y**.
  - **Enable Layer 3 Test** to **n**.
  - **Direct IP-IP Audio Connections to?** to **y**.
  - **Far-end Network Region.** If you set the maximum bandwidth for video calls in an IP network region, assign the appropriate IP network region.
- Optional: Create one incoming signaling group per MGC board in the Polycom MGC system for a secondary CLAN. If the primary CLAN fails, the MGC will use the alternate gatekeeper list as a list of alternate CLANs with which to register.

For outgoing signaling groups, you must:

- Create one outgoing signaling group (LRQ signaling group) per board in the Polycom MGC system for the primary CLAN. This outgoing signaling group is used for outgoing LRQ calls to the co-resident gatekeeper in the Polycom MGC system.

  Keep in mind the following information:

  - For Avaya Communication Manager Release 3.0.1, one signaling group can support a maximum of 31 calls.
  - For Avaya Communication Manager Release 3.1 or later, one signaling group can support a maximum of 255 calls.

- Set the following parameters for the outgoing signaling groups:
  - **IP Video?** to **y**.
  - **Near-end Listen Port** to **1719**.
  - **Far-end Listen Port** to **1719**.
  - **LRQ Required?** to **y**.
  - **Enable Layer 3 Test** to **n**.
  - **Direct IP-IP Audio Connections to?** to **y**.
  - **Far-end Network Region.** If you set the maximum bandwidth for video calls in an IP network region, assign the appropriate IP network region.

  Note:

  Do not set Trunk Group for Channel Selection. If you set this parameter, all incoming video calls may fail or video may close during audio shuffle.

- Optional: Create one outgoing signaling group per board in the Polycom MGC system for the secondary CLAN.
- Optional: Create additional outgoing signaling groups per board in the Polycom MGC system per CLAN for additional CLAN load sharing and additional call capacity.

Group Member Assignments

Keep in mind the following information:

- Group member assignments for the incoming trunk may consist of all incoming signaling groups for the Polycom MGC system.
- Group member assignments for the primary outgoing trunk may consist of all signaling groups defined for multiple CLANs to the one primary board in the Polycom MGC system. **Do not mix Polycom MGC boards**.
- Group member assignments for the secondary outgoing trunk may consist of all signaling groups defined for multiple CLANs to the other boards in the Polycom MGC system.

Outgoing Rules

Keep in mind the following information:

- Change dial plan analysis and uniform dial plan as required to support the Polycom MGC-assigned extension range.
- Add AAR analysis for dial plan extension range for use by the Polycom MGC system. Use **lev0** as the type to force use of the private numbering plan.
- On the route pattern form, add an entry for each outgoing trunk group, and set **LAR** to next. Only one route pattern should be required per Polycom MGC system.
- Regarding digit manipulation, present the digits to the Polycom MGC system in the form of “prefix” plus digits. For example, suppose the Polycom MGC system is administered with the prefix **7**, and there is a five-digit dial plan with **715xx** routing to the Polycom MGC system. You should present the digits **715xx** instead of **15xx**, where **15xx** is the meeting rooms. The Polycom MGC system allows support of multiple prefixes.

MGC Limitations

If you attempt to connect a Polycom MGC to a trunked SIP video device, you should expect audio-only calls. This is a limitation of the MGC. The Polycom RMX does not share this limitation.

Examples

Example 1: S87xx with 2 CLANs/MGC-50 with 2 boards, board redundancy, and no CLAN redundancy

In this example, CLAN1 is chosen as the CLAN for use with the Polycom MGC system. CLAN2 is not used. If CLAN1 fails, the Polycom MGC system will not be allowed to register to CLAN2 and will no longer be able to make incoming or outgoing calls. If the Polycom MGC board IP1 fails, IP2 will continue to be able to make incoming and outgoing calls.

Trunk 1: MGC-A Incoming:

SigGroup 1: CLAN1, IP1; 31 trunk members
SigGroup 2: CLAN1, IP2; 31 trunk members

Trunk 2: MGC-A Outgoing Primary:

SigGroup 3: CLAN1, IP1; 31 trunk members

Trunk 3: MGC-A Outgoing Secondary:

SigGroup 4: CLAN1, IP2; 31 trunk members

Example 2: S87xx with 2 CLANs/MGC-50 with 2 boards, board redundancy, and CLAN redundancy

In this example, CLAN1 is chosen as the primary CLAN for the Polycom MGC system to use, and CLAN2 is a backup. CLAN2 provides backup to CLAN1 for Polycom MGC registration and incoming and outgoing calls. If Polycom MGC board IP1 fails, IP2 will continue to be able to make incoming and outgoing calls.

Note that the incoming signaling groups for CLAN2 will be out-of-service unless the Polycom MGC boards are forced to register with CLAN2 in the event that CLAN1 is unavailable.

Trunk 1: MGC-A Incoming:

SigGroup 1: CLAN1, IP1; 31 trunk members
SigGroup 2: CLAN1, IP2; 31 trunk members
SigGroup 3: CLAN2, IP1; 31 trunk members
SigGroup 4: CLAN2, IP2; 31 trunk members

Trunk 2: MGC-A Outgoing Primary:

SigGroup 5: CLAN1, IP1; 31 trunk members
SigGroup 6: CLAN2, IP1; 31 trunk members

Trunk 3: MGC-A Outgoing Secondary:

SigGroup 7: CLAN1, IP2; 31 trunk members
SigGroup 8: CLAN2, IP2; 31 trunk members

Example 3: S87xx with 2 CLANs/MGC-50 with 3 boards, board redundancy, and CLAN redundancy

In this example, CLAN1 is chosen as the primary CLAN for the Polycom MGC system to use, and CLAN2 is a backup. CLAN2 provides backup to CLAN1 for Polycom MGC registration and incoming and outgoing calls. If Polycom MGC board IP1 fails, IP2 and IP3 will continue to be able to make incoming and outgoing calls.

Note that the incoming signaling groups for CLAN2 will be out-of-service unless the Polycom MGC boards are forced to register with CLAN2 in the event that CLAN1 is unavailable.

T**runk 1: MGC-A Incoming:**

SigGroup 1: CLAN1, IP1; 31 trunk members
SigGroup 2: CLAN1, IP2; 31 trunk members
SigGroup 3: CLAN1, IP3; 31 trunk members
SigGroup 4: CLAN2, IP1; 31 trunk members
SigGroup 5: CLAN2, IP2; 31 trunk members
SigGroup 6: CLAN2, IP3; 31 trunk members

Trunk 2: MGC-A Outgoing Primary:

SigGroup 7: CLAN1, IP1; 31 trunk members
SigGroup 8: CLAN2, IP1; 31 trunk members

Trunk 3: MGC-A Outgoing Secondary:

SigGroup 9: CLAN1, IP2; 31 trunk members
SigGroup 10: CLAN2, IP2; 31 trunk members
SigGroup 11: CLAN1, IP3; 31 trunk members
SigGroup 12: CLAN2, IP3; 31 trunk members

Example 4: S87xx with 4 CLANs/MGC-50 with 3 boards, board redundancy, and outgoing CLAN redundancy

In this example, CLAN1 is chosen as the primary CLAN for the Polycom MGC system to use, and CLAN2 is a backup. CLAN2 provides backup to CLAN1 for Polycom MGC registration and incoming and outgoing calls. If Polycom MGC board IP1 fails, IP2 and IP3 will continue to be able to make incoming and outgoing calls.

Note that the incoming signaling groups for CLAN2 will be out-of-service unless the Polycom MGC boards are forced to register with CLAN2 in the event that CLAN1 is unavailable.

Note that CLAN3 and CLAN4 are not used. Additional outgoing call capacity could be added by defining additional outgoing signaling groups between CLAN3 to IP1, IP2, and IP3, and CLAN4 to IP1, IP2, and IP3. Additional incoming call capacity could be added by defining additional incoming signaling groups between CLAN3 and CLAN4 to boards IP1, IP2, and IP3.

Trunk 1: MGC-A Incoming:

SigGroup 1: CLAN1, IP1; 31 trunk members
SigGroup 2: CLAN1, IP2; 31 trunk members
SigGroup 3: CLAN1, IP3; 31 trunk members
SigGroup 4: CLAN2, IP1; 31 trunk members
SigGroup 5: CLAN2, IP2; 31 trunk members
SigGroup 6: CLAN2, IP3; 31 trunk members

Trunk 2: MGC-A Outgoing Primary:

SigGroup 7: CLAN1, IP1; 31 trunk members
SigGroup 8: CLAN2, IP1; 31 trunk members

Trunk 3: MGC-A Outgoing Secondary:

SigGroup 9: CLAN1, IP2; 31 trunk members
SigGroup 10: CLAN2, IP2; 31 trunk members
SigGroup 11: CLAN1, IP3; 31 trunk members
SigGroup 12: CLAN2, IP3; 31 trunk members

Configure Ad-hoc Video Conferencing for a Polycom MGC Video Conferencing Bridge Platform

This section describes how to configure Ad-hoc video conferencing for a Polycom MGC video conferencing bridge platform. It contains the following sections:

- Limitations
- Checklist
- Configuration Procedures
- Display Capacity for Ad-hoc Video Conferencing
- View Video Conferencing Bridges

Limitations

It is important to note that there are a number of limitations associated with this configuration. In a deployment which uses Polycom Converged Management Application[1] (CMA), conference users cannot establish video if they are added to an Ad-hoc conference. To leverage the full benefits of Ad-hoc video conferencing, Avaya recommends using Avaya Communication Manager 5.0+ in place of Polycom CMA. Ad-hoc video conferencing is only supported on Polycom systems when they are in Avaya mode and registered to Avaya Communication Manager.

Checklist

When setting up Ad-hoc video conferencing for a Polycom MGC, you will need to know the following information:

- the IP codec sets you want to use
- the IP network regions you want use
- the IP address of the IP board for the MGC system
- the IP address of the CLAN

1 Polycom CMA was previously known as Polycom PathNavigator or Polycom ReadiManager SE200.

Configuration Procedures

To configure Ad-hoc conferencing, you must perform the following steps:

1. Configure the IP network regions for the MGC.
2. Configure the MGC for use with an Avaya server.
3. Determine the maximum number of Ad-hoc video conferencing ports your voice system supports.
4. Configure the Class of Service for Ad-hoc video conferencing.
5. Configure a video bridge.
6. Configure the MGC system.

Note:

Keep in mind the following information when configuring the Polycom MGC:

- Place the Polycom MGC in a dedicated network region with a dedicated codec set to infer the conference bit rates.
- Ensure that you specify the correct network region (Far-end Network Region field) when you add the signaling groups for the MGC (Signaling Group form).
- Ensure that all other network regions have direct connectivity to the MGC's network region (**change ip-network-region** command).

Procedure 1: Configure IP Network Regions

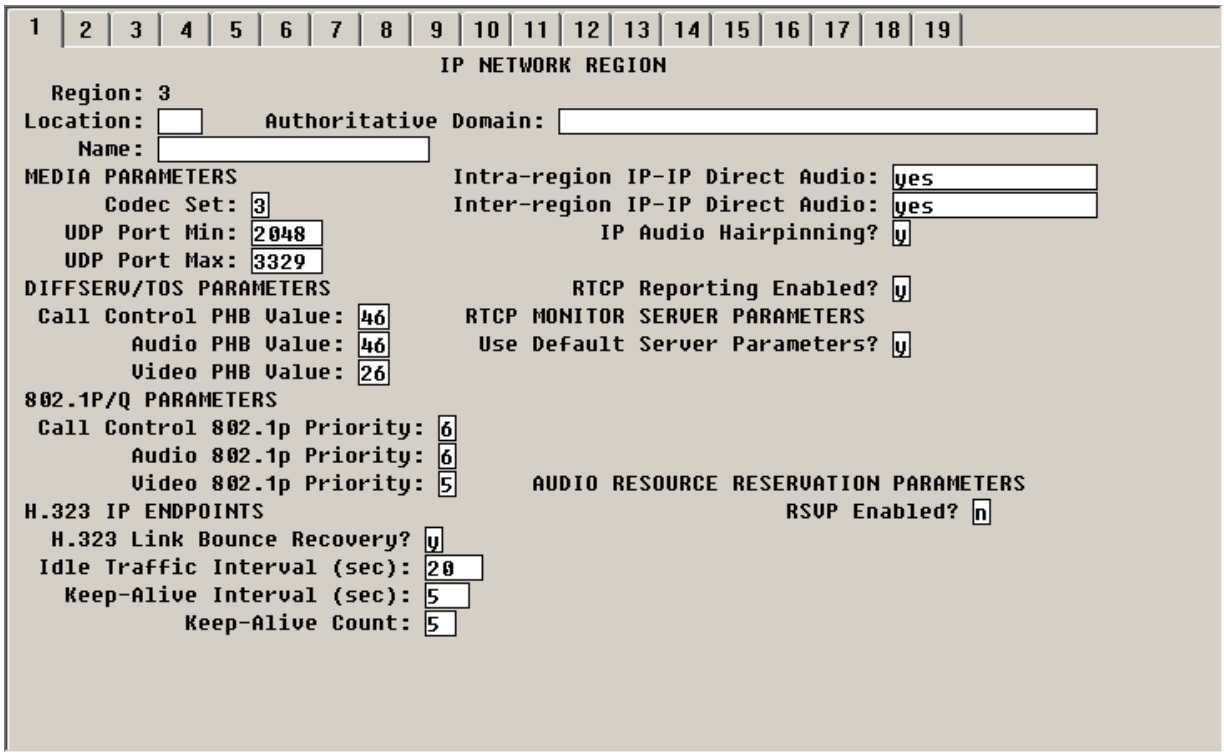
You must place the Polycom MGC in a dedicated network region and ensure that all other network regions have direct connectivity to the Polycom MGC's network region.

To configure the IP network regions:

1. Use the **change ip-network-region *x*** command (where ***x*** is the chosen IP network region) to access the IP Network Region form for the specified region.

   The IP Network Region form appears.

Figure 39: Example of Page 1 of the IP Network Region Form



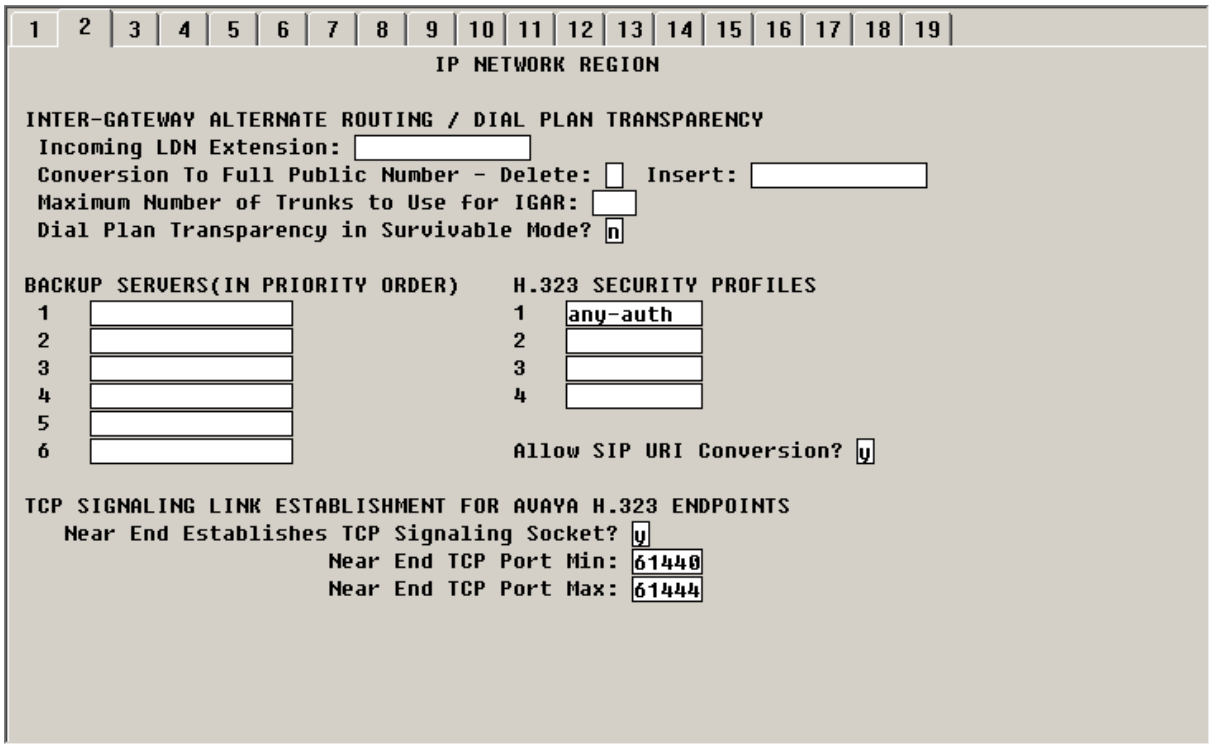
2. Set **Intra-region IP-IP Direct Audio** to **yes**.
3. Set **Inter-region IP-IP Direct Audio** to **yes**.

   Note:

   Shuffling is recommended. However, you can set shuffling to **no**, and video calls will work properly.

4. Go to page 2 of the form.

Figure 40: Example of Page 2 of the IP Network Region Form



5. Set **Security Procedures 1** to **any-auth**.
6. Go to page 3 of the form.
7. Set **codec set** to the appropriate codec set you defined.
8. Set **Video Norm** to the amount of bandwidth that you want to allocate for the normal video pool to each IP network region.
9. Set **Video Prio** to the amount of bandwidth that you want to allocate for the priority video pool to each IP network region.
10. Set **Video Shr**. Specify whether the normal video pool can be shared with the audio pool for each link between IP network regions (**y** or **n**).
11. Repeat Steps 1 through 10 for each IP network region that will be used for video in this system.

Procedure 2: Configure the Polycom RMX for Use with an Avaya Server

Perform the procedures in the appropriate section to configure the Polycom MGC system:

1. Configure a Polycom MGC-25 Video Conferencing Bridge Platform for an Avaya S8300 Server on page 96.
2. Configure Polycom MGC Video Conferencing Bridge Platforms with Avaya S8500 and S87xx Server on page 100.

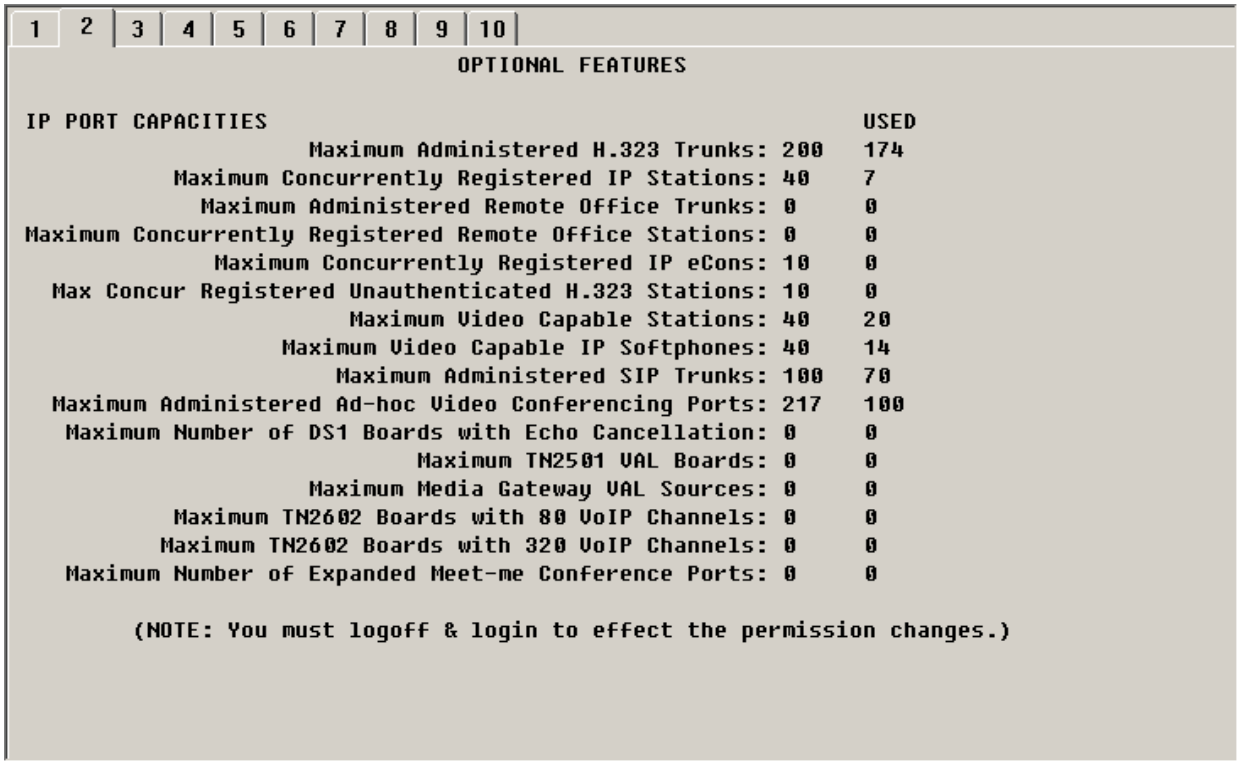
After performing these procedures, go to Procedure 3: Determine the Maximum Number of Ad-hoc Video Conferencing Ports Supported on page 111.

Procedure 3: Determine the Maximum Number of Ad-hoc Video Conferencing Ports Supported

To determine the maximum number of Ad-hoc video conferencing ports your voice system supports:

1. Use the **display system-parameters customer-options** command to access the Optional Features form.
2. On page 2 of the form, verify **Maximum Administered Ad-hoc Video Conferencing Ports**. The maximum number of Ad-hoc video conferencing ports allowed is the number of video ports available for Ad-hoc use on the MCU(s). For example, if you have three MCUs, and each MCU has 16 ports available for Ad-hoc use, the maximum number of Ad-hoc video conferencing ports allowed is 48. This is a license count that Avaya provides based on your stated needs. Licensing and administration are two different decisions on port counts.

Figure 41: Example of Page 2 of the Optional Features Form



In this example, the system can have a maximum of 217 administered Ad-hoc video conferencing ports. Currently, 100 Ad-hoc video conferencing ports are being used.

Procedure 4: Configure Class of Service

To configure the Class of Service for Ad-hoc video conferencing:

1. Use the **change cos** command to access the Class of Service form.
2. Go to page 2 of the form.
3. Set **Ad-hoc Video Conferencing** for the appropriate COS levels.

Procedure 5: Configure a Video Bridge

To configure a video bridge:

1. Use the **add video-bridge *xx*** command (where ***xx*** is the bridge number between 1 to 40, and each video bridge belongs to an MCU) to access the Video Bridge form.

Figure 42: Example of the Video Bridge Form

2. In **Name**, enter the name for this video bridge (for example, *Ad Hoc Video Bridge - MGC25*).
3. Set **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 that are available for Ad-hoc use on the associated MGC based on a needed bit rate for video.
4. In **Trunk Groups**, enter the administered incoming or outgoing ISDN H.323 or SIP trunk groups you added for the MGC. All entries must be of the same carrier type (that is, all H.323 trunks or all SIP trunks).

   The Far End Resource Info, ID Range, Priority Factory Number, and Standard Factory Number fields appear.

   Note:

   MGC Ad-hoc should not be used for SIP video endpoints. Expect no video.
5. Set **Far End Resource Info?** to **n**. The Priority Factory Number and Standard Factory Number fields are removed.

6. Set **ID Range** to the range of ports. These IDs correspond to the actual conference ID numbers of meeting rooms configured on the MGC. For example, if you enter the range 1000 - 1003, you must configure 1000, 1001, 1002, and 1003 as meeting rooms on the MGC. These meeting rooms are for Ad-hoc use only and must not be accessible via the Unified Dial Plan (UDP). Note that Automatic Alternate Routing (AAR) and Unified Dial Plan are not used to connect to these meeting room numbers. Conference IDs (and factory numbers) are completely independent of the dial plan. As a result, you can set up several video bridges with exactly the same conference IDs and numbers. (This will make it easier for you to maintain configurations and swap hardware.)

Procedure 6: Configure the MGC System

On the MGC system, perform the following steps for Ad-hoc conferencing:

1. Create meeting room IDs that correspond to the ID range on Avaya Communication Manager Video Bridge form, with each being video switching auto conferences. Determine the ID length from the MGC system.cfg file.
2. Set 1*1 transcoding so cascaded conferences display properly.

Display Capacity for Ad-hoc Video Conferencing

To display the 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.)

View Video Conferencing Bridges

Use the **list video-bridge** command to view the video conferencing bridges administered on your system.

Configure an Avaya Meeting Exchange 5.1 S6800 Bridge

This section describes how to configure an Avaya Meeting Exchange 5.1 S6800 bridge as an external video bridge.

Checklist

When setting up an Avaya Meeting Exchange 5.1 S6800 bridge, you will need to know the following information:

- the IP codec sets you want to use
- the IP network regions you want use
- the Priority Factory Number and the Standard Factory Number to use in the Avaya Communication Manager system and the Avaya Meeting Exchange bridge.

Things to Keep in Mind

Before configuring an Avaya Meeting Exchange 5.1 S6800 bridge, keep in mind the following information:

- For more information on the Avaya Meeting Exchange bridge, refer to the *Avaya Meeting Exchange 5.1 Installation Guide for S6X00 Servers*. This document is available on support.avaya.com.
- Ad-hoc supports six audio callers per conference.
- Schedule supports 16 video callers per Meeting Exchange 5.1 scheduled conference.
- Each 6800 bridge can support up to 2000 video ports
- Each conference can support up to 16 video participant.
- The Meeting Exchange audio conferencing server supports video from version 5.1 onwards. If you upgrade from Meeting Exchange 5.0 to Meeting Exchange 5.1, you must undetake a manual configuration process. For more information on the manual configuration process, see Configuration Procedures on page 116.
- The configuration process is the same Whether you configure a single instance of Communication Manager or multiple instances of Communication Manager with the Meeting Exchange video solution.
- The video capacity for each Convedia MPC varies depending on bit rate, picture size, and frame rate. See the following table.

Table 11: Video Capacity

Total Bit Rate	Picture SIze (MPI)	Audio Codec	# Ports per MPC	Resource Allocation for Video (%)
768 Kbit/s	CIF:1	G.711	45	91
384 Kbit/s	CIF:2	G.711	90	75
128 Kbit/s	QCIF:4	G.711	250	75

Configuration Procedures

To configure an Avaya Meeting Exchange 5.1 S6800 bridge with an Avaya Communication Manager system, you must perform the following steps:

1. Verify the licensing on the Avaya Communication Manager system.
2. Configure IP network regions for the Meeting Exchange system.
3. Add an entry in the IP node names for the Meeting Exchange system.
4. Add a signaling group for the Meeting Exchange system.
5. Add a SIP trunk group for the Meeting Exchange system.
6. Configure the Avaya Meeting Exchange 5.1 S6800 bridge.
7. Configure the Radisys CMS 6000 for Avaya Meeting Exchange 5.1 S6800 bridge.
8. Configure Avaya Communication Manager Video Bridge (Ad-hoc conferencing only).
9. Configure Avaya Communication Manager to use SES for Avaya Meeting Exchange.

Procedure 1: Verify Licensing

You must verify that the Avaya Communication Manager system is licensed for video endpoints, Ad-hoc video conferencing ports, and multimedia IP SIP trunking.

To verify licensing:

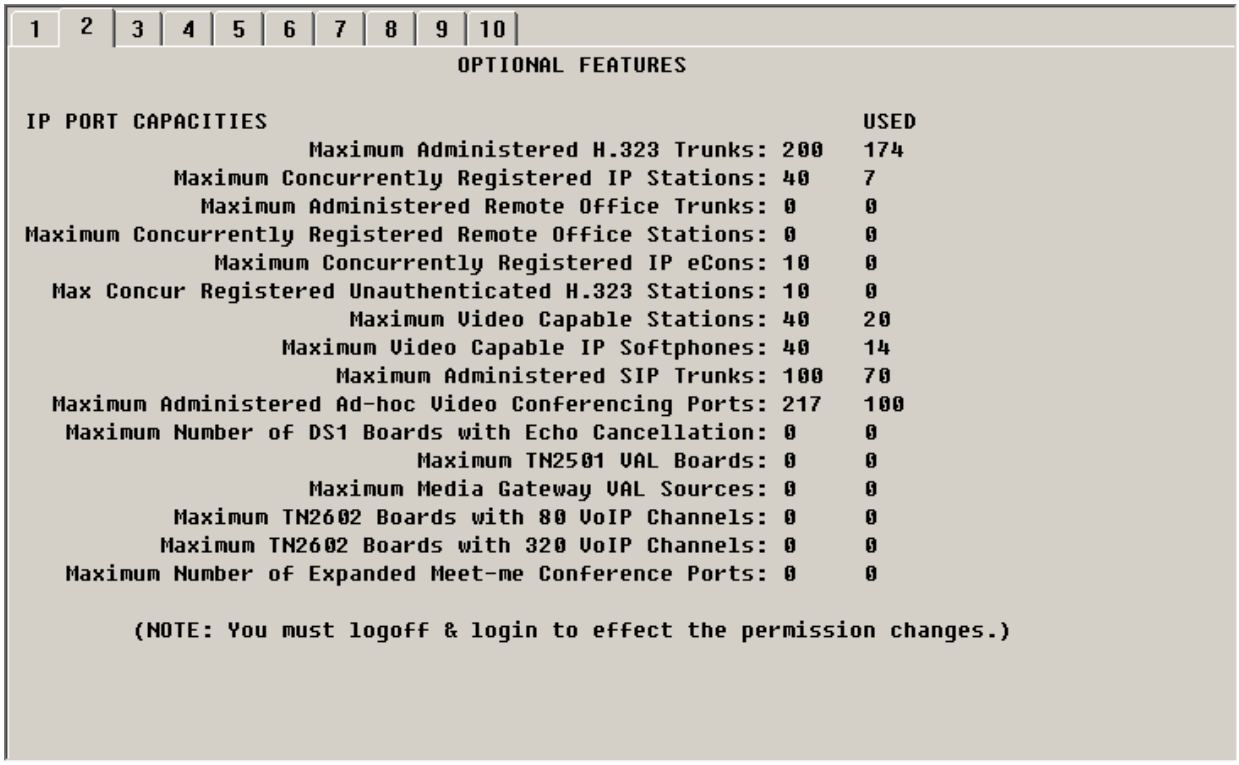
1. Use the **display system-parameters customer-options** command to access the Optional Features form.
2. On page 2 of the form, verify the following settings:
   - **Maximum Video Capable IP Softphones**. This number is provided by the RFA license file.

   Note:

   To provide video softphone capability, you must have at least this number of IP Softphone licenses. Page 10 of this form displays the number of IP Softphone licenses you have.

   - **Maximum Administered Ad-hoc Video Conferencing Ports**. The maximum number of Ad-hoc video conferencing ports allowed is the number of video ports available for Ad-hoc use on the MCU(s). For example, if you have three MCUs, and each MCU has 16 ports available for Ad-hoc use, the maximum number of Ad-hoc video conferencing ports allowed is 48.

Figure 43: Example of Page 2 of the Optional Features Form



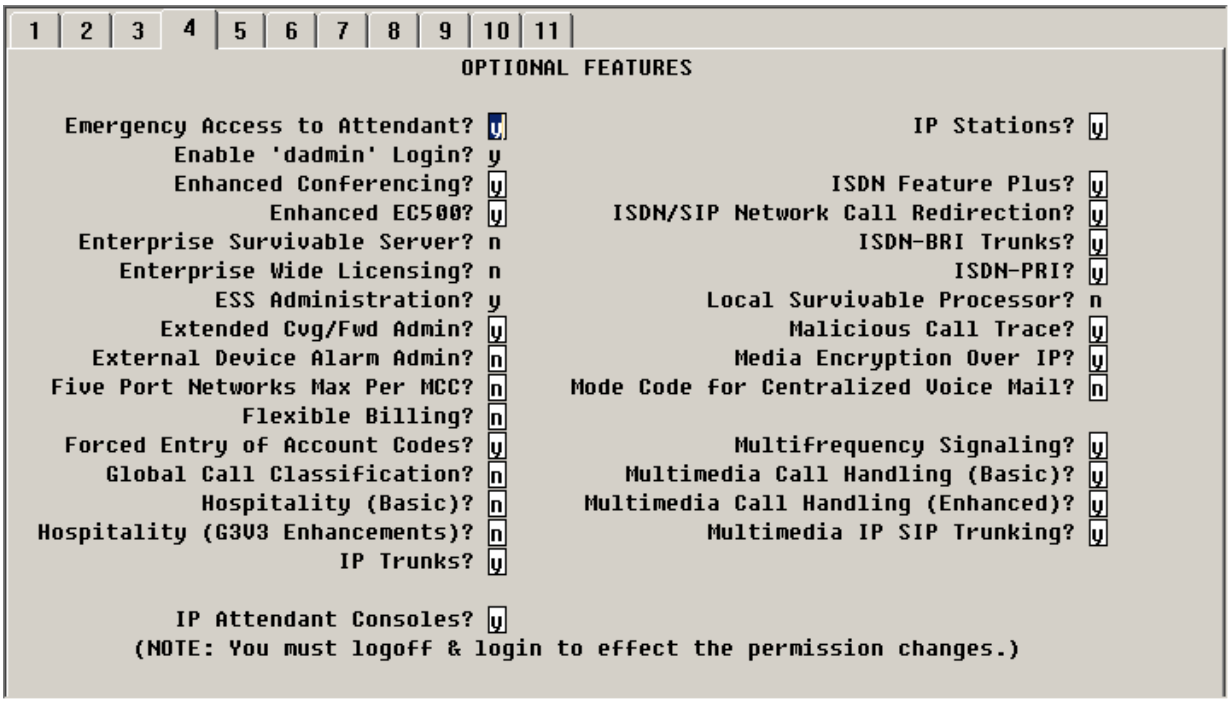
```
1  2  3  4  5  6  7  8  9  10
                        OPTIONAL FEATURES

IP PORT CAPACITIES                                          USED
                    Maximum Administered H.323 Trunks: 200  174
          Maximum Concurrently Registered IP Stations: 40   7
            Maximum Administered Remote Office Trunks: 0    0
Maximum Concurrently Registered Remote Office Stations: 0   0
             Maximum Concurrently Registered IP eCons: 10   0
  Max Concur Registered Unauthenticated H.323 Stations: 10   0
                       Maximum Video Capable Stations: 40   20
                  Maximum Video Capable IP Softphones: 40   14
                      Maximum Administered SIP Trunks: 100  70
  Maximum Administered Ad-hoc Video Conferencing Ports: 217  100
   Maximum Number of DS1 Boards with Echo Cancellation: 0    0
                             Maximum TN2501 VAL Boards: 0    0
                    Maximum Media Gateway VAL Sources: 0    0
          Maximum TN2602 Boards with 80 VoIP Channels: 0    0
         Maximum TN2602 Boards with 320 VoIP Channels: 0    0
   Maximum Number of Expanded Meet-me Conference Ports: 0    0

       (NOTE: You must logoff & login to effect the permission changes.)
```

In this example, the system can have:

- a maximum of 40 video-enabled Avaya IP Softphones. Currently, 13 video-capable Avaya IP Softphones are being used.
- a maximum of 217 administered Ad-hoc video conferencing ports. Currently, 100 Ad-hoc video conferencing ports are being used.

3. Go to page 4.

Figure 44: Example of Page 4 of the Customer-Options Form



```
 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
                        OPTIONAL FEATURES

  Emergency Access to Attendant? y                        IP Stations? y
          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                           ISDN-PRI? y
             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? y             Multifrequency Signaling? y
     Global Call Classification? n       Multimedia Call Handling (Basic)? y
            Hospitality (Basic)? n    Multimedia Call Handling (Enhanced)? y
Hospitality (G3V3 Enhancements)? n            Multimedia IP SIP Trunking? y
                     IP Trunks? y

          IP Attendant Consoles? y
       (NOTE: You must logoff & login to effect the permission changes.)
```

4. Make sure **Multimedia IP SIP Trunking?** is set to **y**.

Procedure 2: Configure IP Network Regions

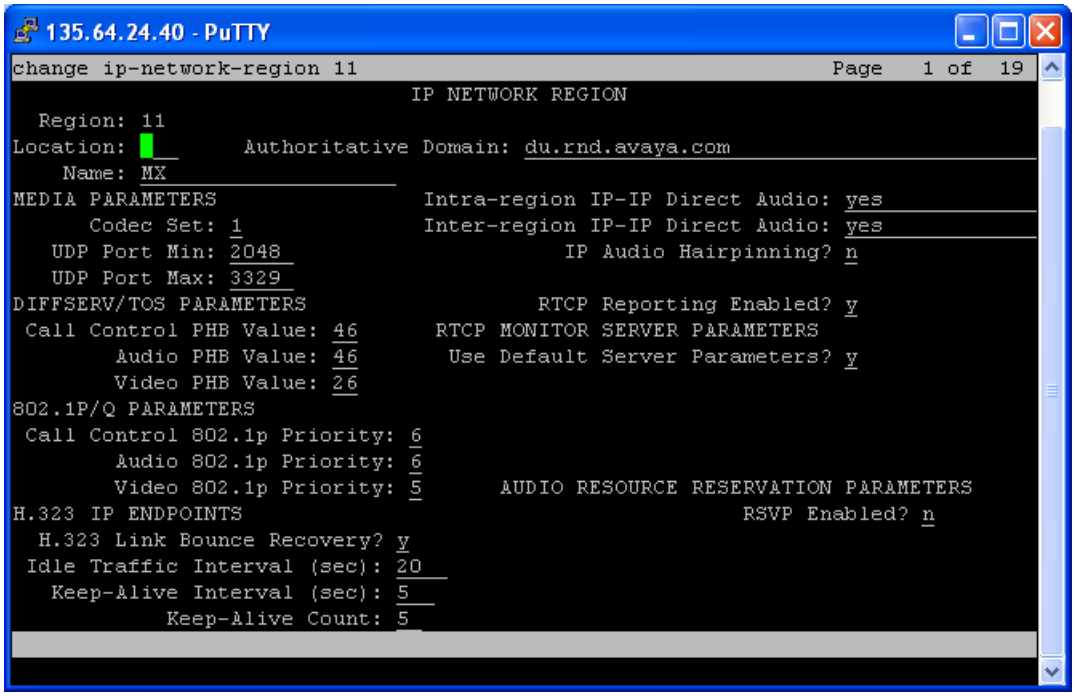
You must place the Meeting Exchange system in a dedicated network region and ensure that all other network regions have direct connectivity to the Meeting Exchange system's network region.

To configure the IP network regions:

1. Use the **change ip-network-region *x*** command (where ***x*** is the chosen IP network region) to access the IP Network Region form for the specified region.

   The IP Network Region form appears.

Figure 45: Example of Page 1 of the IP Network Region Form



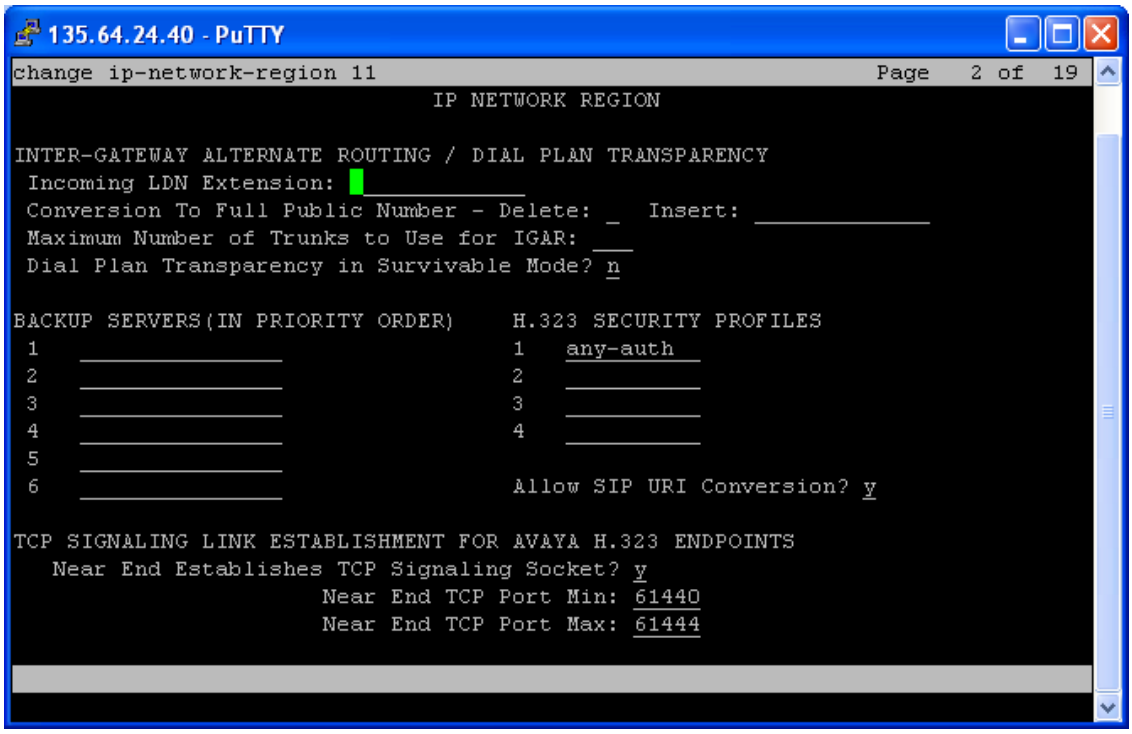
2. Set **Authoritative Domain** for IP network regions that contain SIP endpoints/MCUs.
3. Set **Intra-region IP-IP Direct Audio** to **yes**.
4. Set **Inter-region IP-IP Direct Audio** to **yes**.

   Note:

   Shuffling is recommended. However, you can set shuffling to **no**, and video calls will work properly.

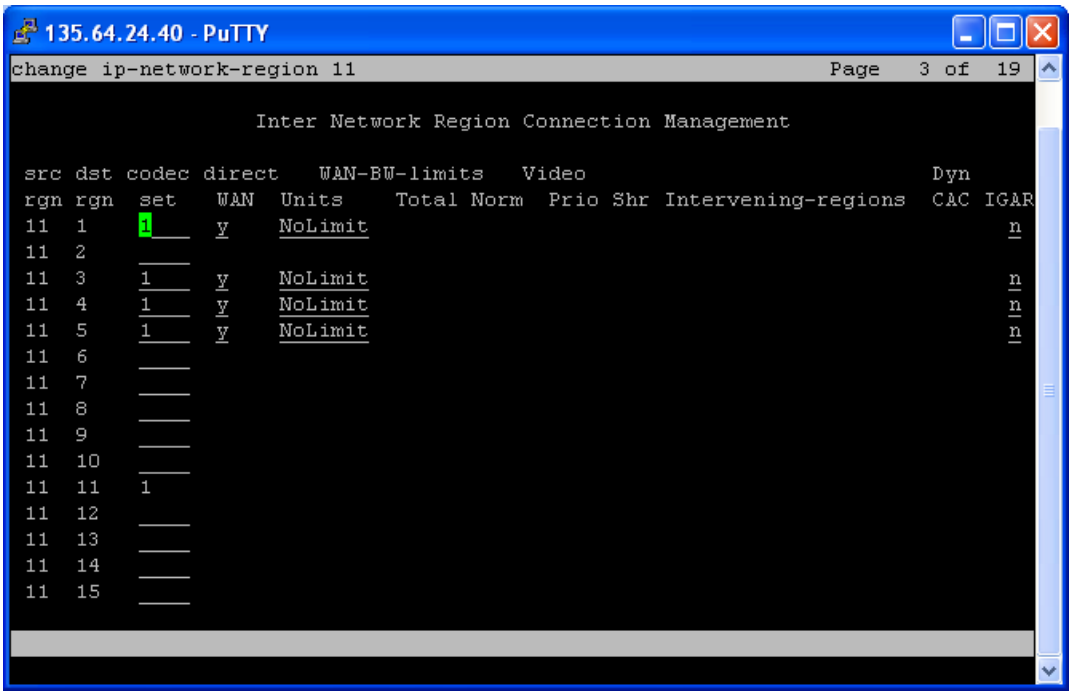
5. Go to page 2 of the form.

Figure 46: Example of Page 2 of the IP Network Region Form



6. Set **H.323 SECURITY PROFILES 1** to **any-auth**.
7. Go to page 3 of the form.

Figure 47: Example of Page 3 of the IP Network Region Form



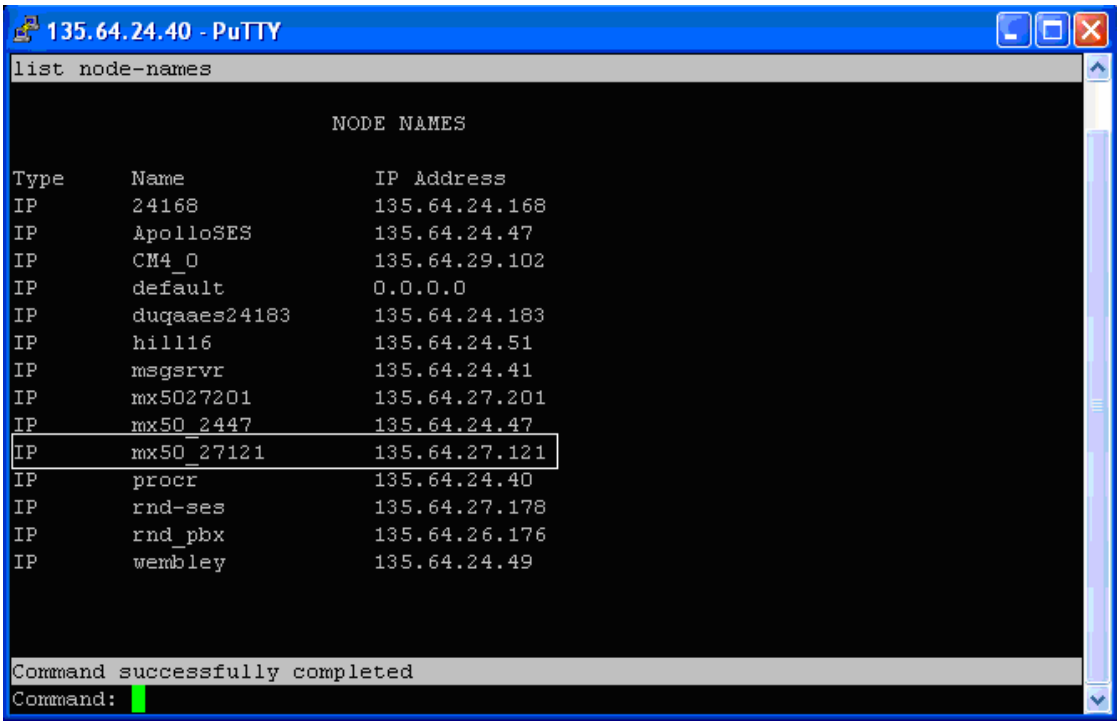
8. Set **codec set** to the appropriate codec set you defined.
9. Set **Units** to **NoLimit** for each destination IP network region. You can set unlimited bandwidth or use the bandwidth management option by restricting the bandwidth.
10. Repeat Steps 1 through 9 for each IP network region that will be used for video in this system.

Procedure 3: Add an Entry in the IP Node Names for the Meeting Exchange System

To add an entry in the IP Node Names form for the Meeting Exchange system:

1. Use the **change node-names ip** command to access the IP Node Names form.

Figure 48: Example of Page 1 of the IP Node Names Form



2. In the **Name** field, enter a name for the Meeting Exchange S6200 system.
3. In the corresponding **IP Address** field, enter the IP address of the Meeting Exchange Application server.

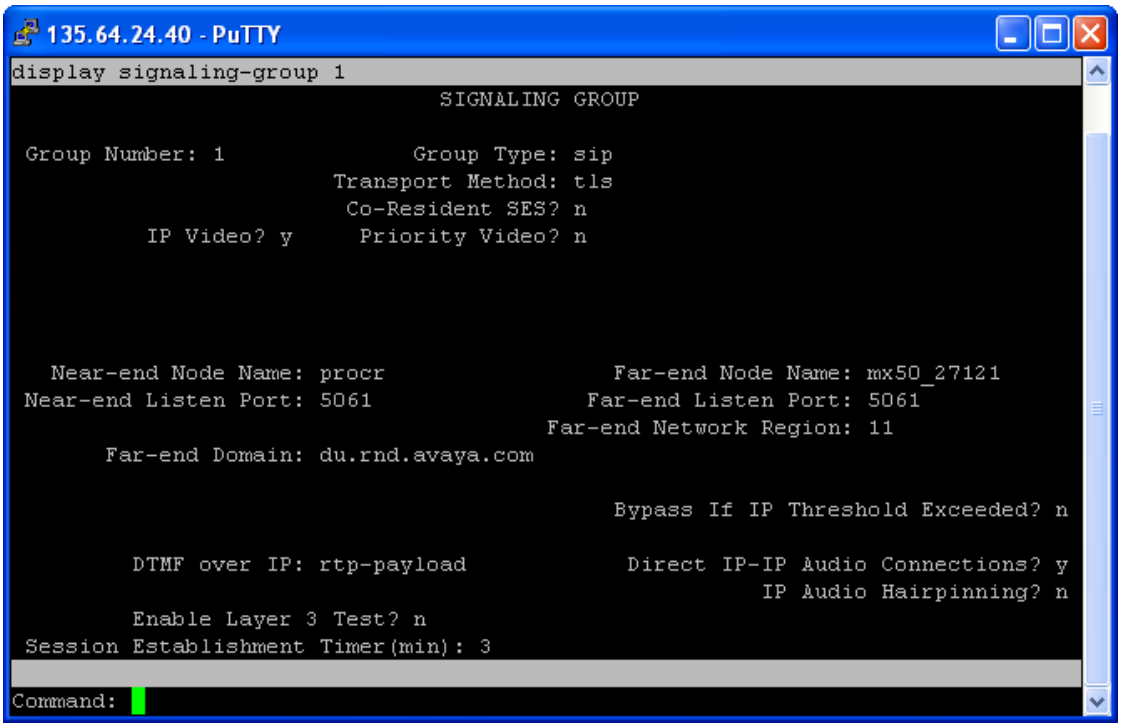
Procedure 4: Add a Signaling Group for the Meeting Exchange System

To add a signaling group for the Meeting Exchange system:

1. Use the **add signaling-group *xx*** command (where ***xx*** is the chosen signaling group) to access the Signaling Group form.

   The Signaling Group form appears.

Figure 49: Example of Page 1 of the Signaling Group Form



2. Set **Group Type** to **sip**.
3. Set **Transport Method** to **tls** or **tcp**.
4. Set **IP Video** to **y**.
5. Set **Priority Video** as appropriate.
6. Set **Near-end Node Name**. For example, for an S8300 system, you would enter ***procr***. For an S8500 or S8700 system, you would enter the name of the CLAN board.
7. Set **Near-end Listen Port** to **5061** or **5060**.
8. Set **Far-end Node Name** to the name you entered for the Meeting Exchange system.
9. Set **Far-end Listen Port** to **5061** or **5060**.
10. Set **Far-end Network Region** to the network region you specified for the Meeting Exchange system.
11. Set **Session Establishment Timer (min)** to **120**.
12. Set **DTMP over IP** to **rtp-payload**.
13. Set **Enable Layer 3 Test** to **n**.
14. Set **Direct IP-IP Audio Connected** to **y**.

Procedure 5: Add a SIP Trunk Group for the Meeting Exchange System

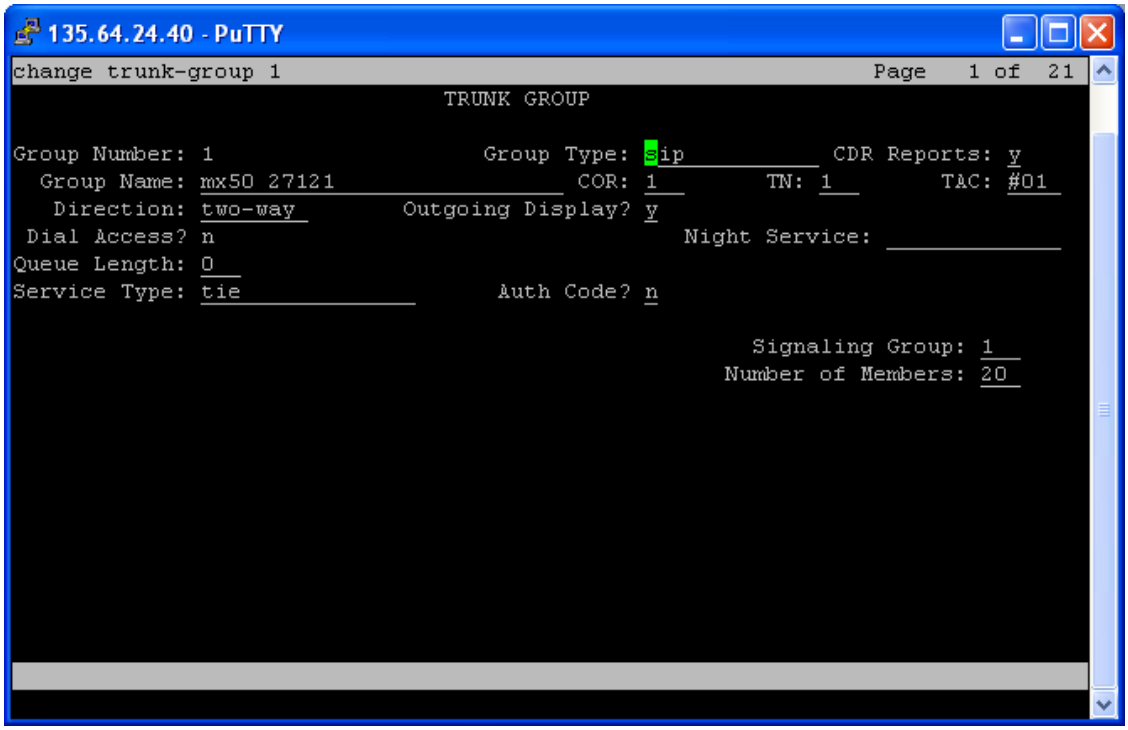
You must administer a SIP trunk group for the Meeting Exchange system.

Perform the following steps:

1. Use the **add trunk-group *xx*** command (where ***xx*** is the chosen trunk group) to access the Trunk Group form.

   The Trunk Group form appears.

Figure 50: Example of Page 1 of the Trunk Group Form



a. Set **Group Type** to **sip**.

b. Set **Group Name** to the name of the Meeting Exchange system (for example, Avaya Meeting Exchange 5.1 SIP Bridge).

c. Set **COR**.

d. Set **Direction** to **two-way**.

e. Set **Outgoing Display** to **y** to display caller ID (from the Station form).

f. Set **Service Type** to **tie**.

g. Set **Signaling Group** to the signaling group you created for the Meeting Exchange system.

h. Set **Number of Members**.

Procedure 6: Configure the Avaya Meeting Exchange 5.1 S6800 Bridge

In this section, you will:

1. Configure the Meeting Exchange bridge for TLS or TCP so it will be able to communicate with Avaya Communication Manager.
2. Configure the non-Ad-hoc video conferencing parameters for the Meeting Exchange bridge.
3. Configure the call branding digits that you will use to dial into the Meeting Exchange bridge.
4. Configure the dial outs for the Meeting Exchange bridge.
5. Configure Avaya Meeting Exchange 5.1 for Radisys CMS 6000.
6. Configure the Ad-hoc video conferencing parameters on the Meeting Exchange bridge.
7. Schedule conferences on Avaya Meeting Exchange 5.1 to ensure correct operation.

Note:

You must log into the Meeting Exchange bridge using ssh with craft and su to sroot. All configuration changes except cbutil require a system reboot for the changes to take effect.

To configure the Meeting Exchange bridge:

1. Using a text editor, open the file /usr/ipcb/config/system.cfg, and make sure the following parameters are configured:
   - MyListener
   - respContact
   - MaxChannelCount
   - MaxVideoChannelsAllowed

   The following is an example of a TLS configuration:

   # ip address of the server
   IPAddress=xxx.xxx.xxx.xxx
   #request we will be listening to
   #TLS
   MyListener=sip:6000@xxx.xxx.xxx.xxx:5061;transport=tls
   #TLS
   respContact=<sip:6000@xxx.xxx.xxx.xxx:5061;transport=tls>
   #Audio port licensing depends on customer
   MaxChannelCount=750
   # video port licensing depends on customer
   MaxVideoChannelsAllowed=125

The following is an example of a TCP configuration:

# ip address of the server
IPAddress=xxx.xxx.xxx.xxx
#request we will be listening to
MyListener=sip:6000@xxx.xxx.xxx.xxx:5060;transport=tcp
#if this setting is populated will Overwrite the contact field in responses
respContact=<sip:6000@xxx.xxx.xxx.xxx:5060;transport=tcp>
#Audio port licensing depends on customer
MaxChannelCount=750
video port licensing depends on customer
MaxVideoChannelsAllowed=125

2. Using a text editor, open the file /usr/ipcb/config/mediaServerInterface.cfg, and make sure the following parameters are configured:

   - EnableVideoSupport

     Valid entries are 0 (off) and 1 (on). The default is 0.

   - VideoSI

     This parameter sets the switching interval. Valid entries are 1 through 10 seconds. The default is 2.

   - VideoSpeakersees

     Valid entries are current and previous. The default is previous.

   - VideoSize

     Valid entries are CIF and QCIF. The default is CIF.

   - VideoBandwidth

     Valid entries are 128, 192, 256, 384, 512, and 768 Kbit/s. The default is 384 Kbits/s.

   - VideoMPI

     This parameter sets the minimum picture interval. Valid entries are 1 through 32. The default is 4. (VideoMPI=1 equals 30 fps.)

The following is an example of the mediaServerInterface.cfg settings:

#Audio recording server
NFSServerIPAddress=xxx.xxx.xxx.xxx
MediaServerIP_1=xxx.xxx.xxx.xxx
MediaServerName_1=mpc2
MediaServerInterfaceSipListenPort_1=5050
# Video Params
# Set EnableVideoSupport to ’1’ to enable video support and ’0’ to disable
EnableVideoSupport=1
VideoSI=2
VideoSpeakersees=previous
VideoSize=CIF
VideoBandwidth=384
VideoMPI=4

3. At the command prompt, type **cbutil add** to add the call branding digits that you use to dial into the bridge. You can configure:
   - SCAN to prompt the user for conference codes.
   - DIRECT to go directly into a pre-configured conference.

   Example:

   cbutil add 24049 0 301 1 n DIRECT -1 Adhoc in Avaya

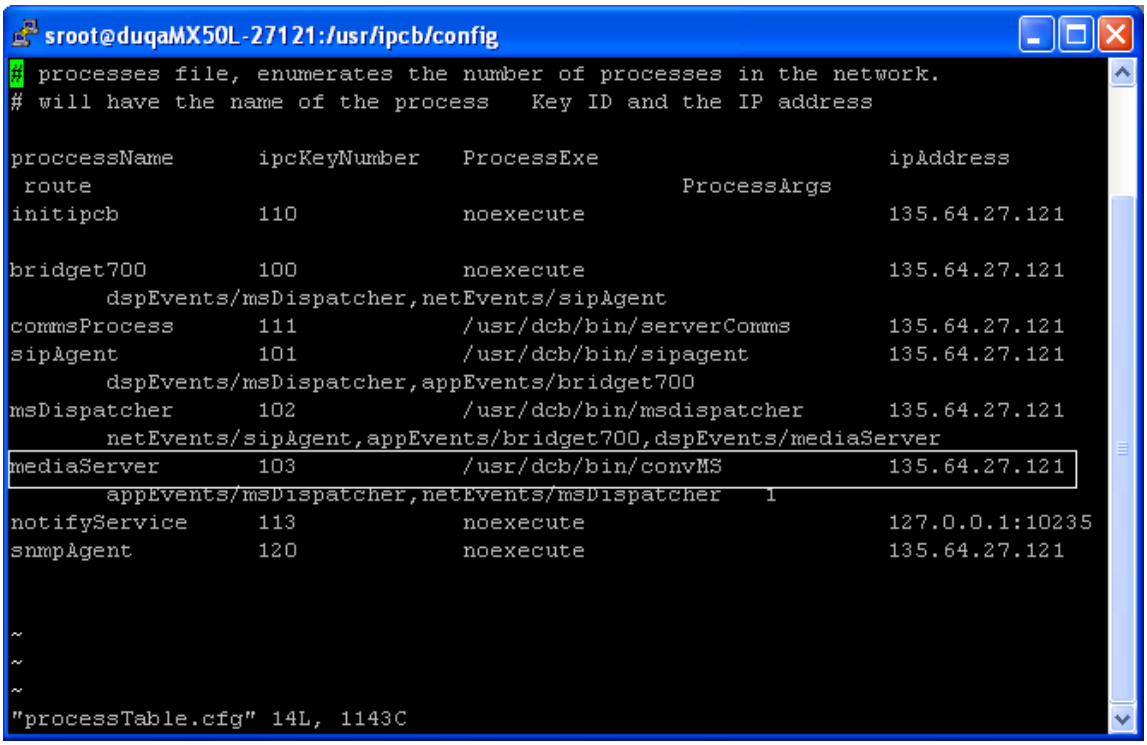
DNIS	Grp	Msg	PS	CP	Function	Line Name	Company Name
24047	0	247	1	N	SCAN	Schedule	Avaya
24049	0	301	1	N	DIRECT	Adhoc	Avaya

4. Using a text editor, open the file /usr/ipcb/config/telnumToURI.tab to configure the dial outs for the Meeting Exchange bridge. Your dial outs are configured on the bridge in /usr/ipcb/config/telnumToURI.tab. See the following example:

TelnumPattern	TelnumConversion	comment
*	"<sip:$1@<proxyipaddress>:5061;transport=tls>"	SES Proxy
40???	"<sip:$1<clan_address>:5061;transport=tls>"	ACM

5. Using a text editor, open the file /usr/ipcb/config/processTable.cfg to configure Avaya Meeting Exchange 5.1 for Radisys CMS600. The convMS process implements the Radisys CMS600 media server interface. See the following figure for an example of the processTable.cfg file.

Figure 51: Example of processTable.cfg File



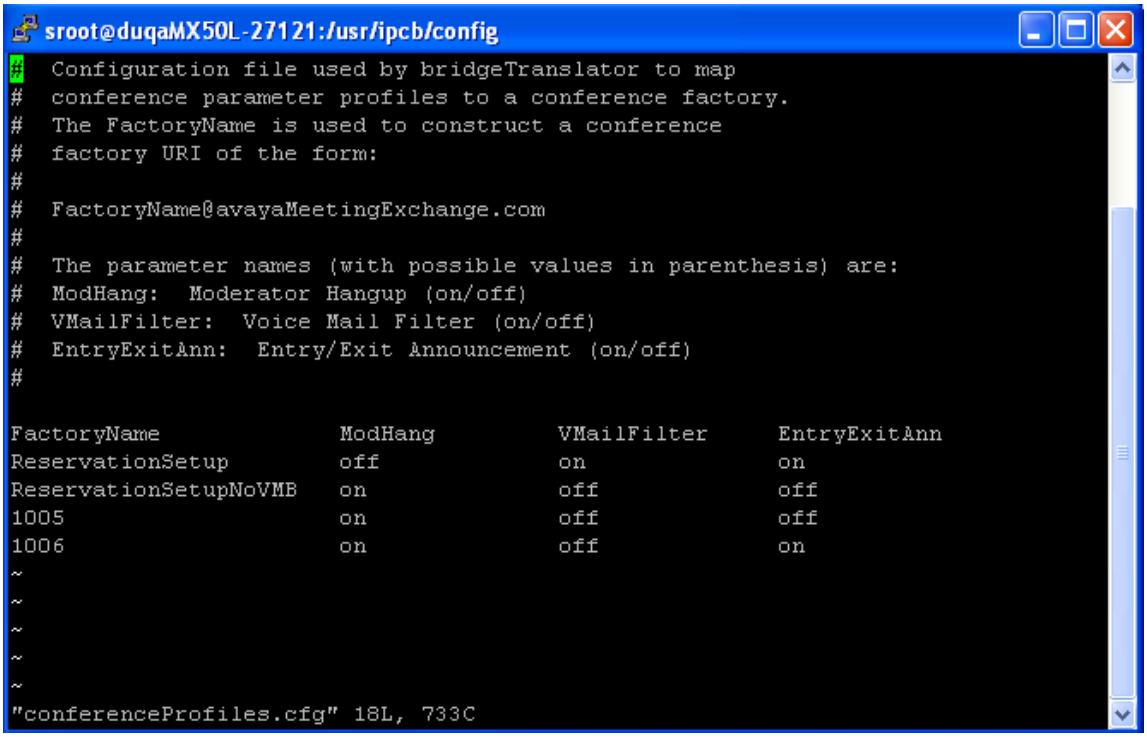
6. Perform the following steps to configure the Ad-hoc video conferencing parameters on the Meeting Exchange bridge:
   a. On Avaya Meeting Exchange 5.1, configure the following values in the file usr/ipcb/config/system.cfg:
      - AdhocConferenceURIPattern
      - AdhocMinPortsAvailable
      - AdhocDefaultConferenceSize
      - RAINotificationInterval
      - RAIHighThreshold
      - RAILowThreshold
      - MaxRAISubscribers

The following is an example of the system.cfg settings:

```
#Adhoc conference parameters
#AdhocConferenceURIPattern=<sip:AdhocDirect$1@$2>
AdhocConferenceURIPattern=<sip:A$1@$2:5061;transport=tls>
AdhocMinPortsAvailable=20
AdhocDefaultConferenceSize=6

#RAI configuration fields

# the interval in seconds at which an RAI notification is sent
# (default 60s, min 1s, max 300s)
RAINotificationInterval=60

# the upper threshold in percentage of total ports at which an
# "AlmostOutOfResources=TRUE" notification is sent
# (default 90%)
RAIHighThreshold=90

# the lower threshold in percentage of total ports at which an
# "AlmostOutOfResources=FALSE" notification is sent
# (only to clear a previous "AlmostOutOfResources=TRUE" notification)
# (default 75%)
RAILowThreshold=75

# the maximum number of RAI subscribers allowed
# (default 10 subscribers, min 0, max 10)
maxRAISubscribers=10
```

b. On Avaya Meeting Exchange 5.1, configure the following values in the file usr/ipcb/config/conferenceProfiles.cfg. See the following figure for an example of the conferenceProfiles.cfg file.

Figure 52: Example of conferenceProfiles.cfg File



Note:

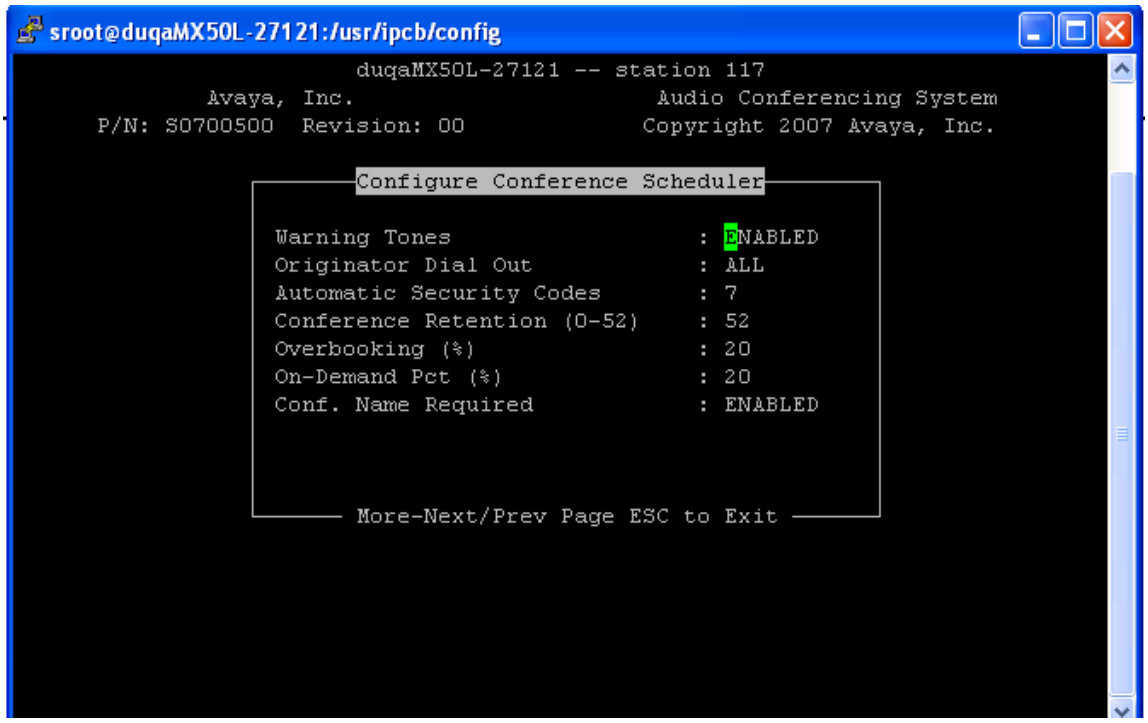
The factory settings 1005 and 1006 should be the same on the Avaya Communication Manager system (Priority Factory number=1005, Standard Factory number=1006).

c. On Meeting Exchange 5.1, from sroot go to dcbmaint 116, select **System Maintenance main menu>Administration menu>Conference Scheduler**, and set:

- **Automatic Security Codes** to **7**.
- **On-Demand Pct (%)** as per ***customer*** requirement. (This is a percentage of all ports used for on-demand and Ad-hoc conferences.)

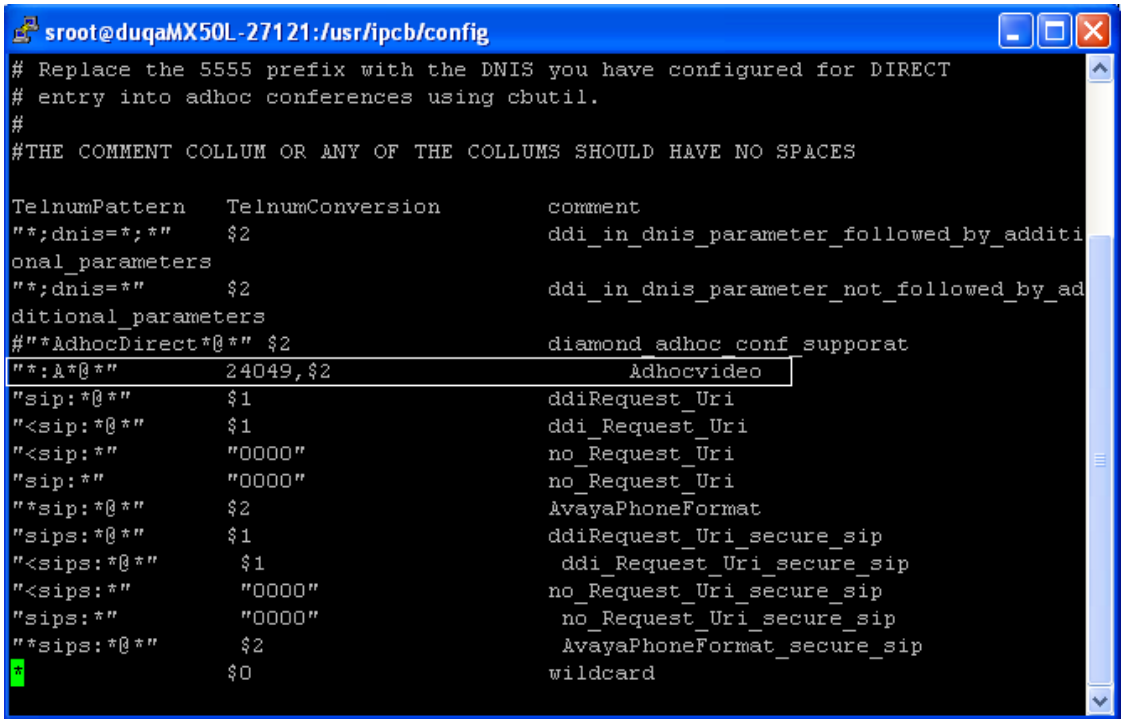
See the following figure for an example of the Configure Conference Scheduler settings.

Figure 53: Example of Configure Conference Scheduler Settings



d. On Avaya Meeting Exchange 5.1, configure the file usr/ipcb/config/UriToTelnum.tab for DNIS. This DNIS entry is used for creating an Ad-hoc conference. 24049 is DNIS for Ad-hoc. The same DNIS has to be in cbutil as DIRECT. (Refer to the cbuilt section.) See the following figure for an example of the UriToTelnum.tab file.

Figure 54: Example of UriToTelnum.tab File



7. Schedule conferences on Avaya Meeting Exchange 5.1.

   Configuring Resources On-Demand

   To enable FLEX conferences:

   a. Connect via ssh to the bridge.

   b. At the command prompt, type **featcfg +flex**.

   c. At the command prompt, type **dcbmaint 115**.

   d. Select **Administration Menu>Configure Scheduler**.

   e. Use the Page Down key to go to the second page.

   f. Set **On-Demand Pct (%)** (for example, 50).

Scheduling Conferences

There are two methods to schedule a conference on the bridge.

- Method 1
  a. Connect via ssh to the bridge.
  b. At the command prompt, type **dcbsched 116**.
  c. Select **Schedule Conference**.
  d. Schedule your conference.
  e. When finished, press the Esc key.
- Method 2

  Install the BridgeTalk application, which is a GUI scheduler that enables you to see your active conferences easily. If you are going to use BridgeTalk, you must first configure a sign-in on the bridge.

  a. Connect via ssh to the bridge.
  b. At the command prompt, type **dcbmaint 11**5.
  c. Choose **Administration Menu>Sign-In Management**, and create a sign-in.
  d. When finished, press the Esc key.
  e. Choose **View>Conference Scheduler** from the toolbar to access the Conference Scheduler. In order for you to perform any operator tasks (such as record/playback, conference listen, and accessing lines from Enter or Help Queues), you must establish an audio path.
  f. Choose **Line>Audio Path** from the BridgeTalk toolbar.
  g. Enter the number for the Operator phone to which you want to dial out. This phone must be configured on the bridge in the file /usr/ipcb/config/telnum/ToURI.cfg similar to the following example:

TelnumPattern	TelnumConversion	comment
40???	"<sip:$1<clan_address>:5061;transport=tls>"	ACM

  In this example, you would dial 2020 from BridgeTalk to establish this Avaya IP phone an the Operator audio path.

Procedure 7: Configure the Convedia CMS 6000 for Avaya Meeting Exchange 5.1 S6800

Note:

You must have administrator permission to edit the configuration and reboot the system for the changes to take effect.

To configure the Convedia CMS 6000:

1. Select **Configuration>Slot Configuration>Configure Video**.

Figure 55: Example of Configure Video Page

2. From the Slot number for the card drop-down list box, select the MPC slot.
3. Set the following parameters in the Configure Video dialog box:
   - **Video MTU** to **1492**.
   - **Video Maximum Desired Bandwidth** to **768**.
   - Enable the **SIP-INFO** check box in **Video I-Frame Request Method(s)**.

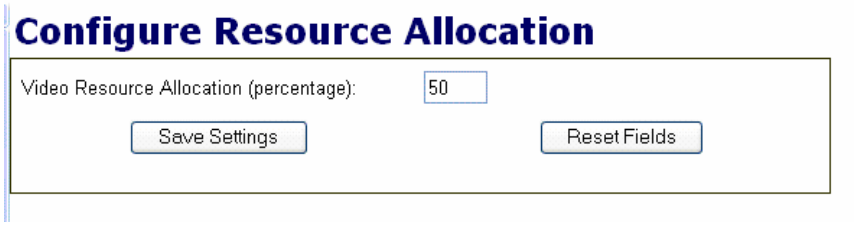
Figure 56: Example of Configure Video Settings

4. In the Configure Video Codec List dialog box, set the following parameters for Entry #1:
   - **Codec** to **H.263**.
   - **Picture Size** to **CIF**.
   - **MPI** to **1**.

Figure 57: Example of Configure Video Codec List Settings

5. In the Configure Resource Allocation dialog box, set **Video Resource Allocation (percentage)** to **50**. When resources are set to 50 percent, and the MPC contains 50 ports, 25 ports are set for video, and 25 ports are set for audio.

Figure 58: Example of Configure Resource Allocation Settings



Example:

1 MPC = 750 callers

50% video on MPC = 125 (Maximum video allowed per MPC = 250 > 128 bit rate)

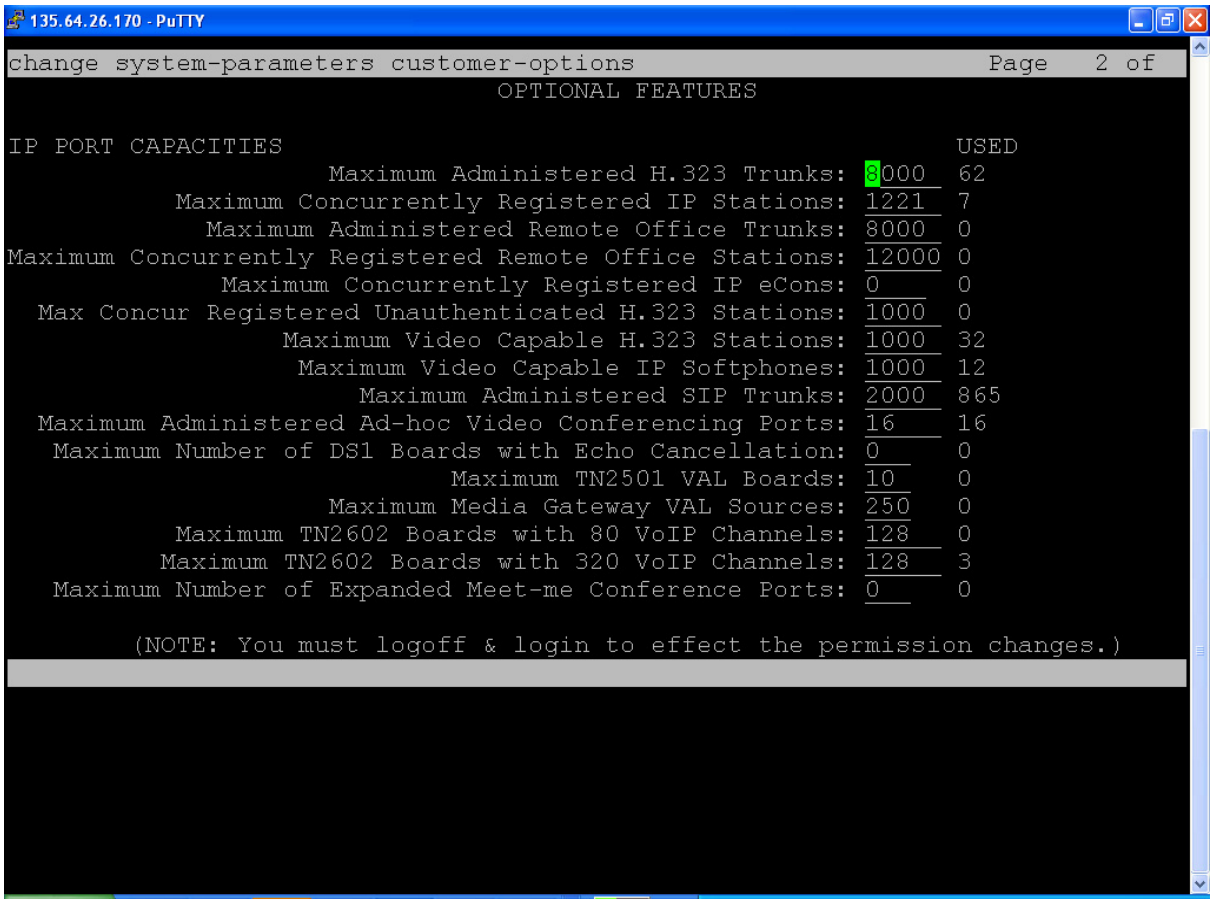
Total audio callers can use: 375 - 125 = 250

Procedure 8: Configure Ad-hoc Conferencing on Avaya Communication Manager

To configure Ad-hoc conferencing on the Avaya Communication Manager system:

1. Perform the following steps to administer Ad-hoc video ports on the Avaya Communication Manager system:
   a. Use the **display system-parameters customer-options** command to access the Optional Features form.
   b. On page 2 of the form, verify **Maximum Administered Ad-hoc Video Conferencing Ports**. The maximum number of Ad-hoc video conferencing ports allowed is the number of video ports available for Ad-hoc use on the MCU(s). For example, if you have three MCUs, and each MCU has 16 ports available for Ad-hoc use, the maximum number of Ad-hoc video conferencing ports allowed is 48.

Figure 59: Example of Page 2 of the Optional Features Form

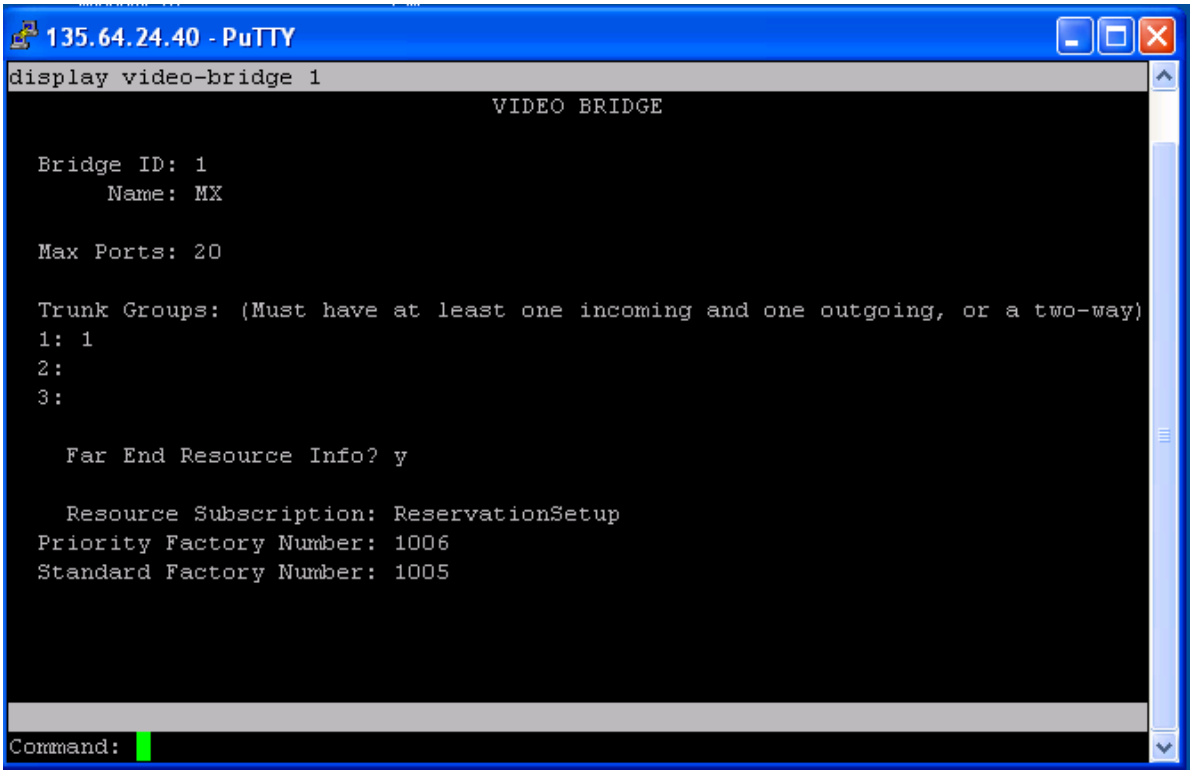


2. Perform the following steps to configure COS for the video ad-hoc-enabled users:
   a. Use the **change cos** command to access the Class of Service form.
   b. Go to page 2 of the form.
   c. Set **Ad-hoc Video Conferencing** for the appropriate COS levels.
3. Perform the following steps to configure a video bridge on the Avaya Communication Manager system:
   a. Use the **add video-bridge *xx*** command (where ***xx*** is the bridge number between 1 to 40) to access the Video Bridge form.
   b. In **Name**, enter the name for this video bridge (for example, *Ad Hoc Video Bridge - Meeting Exchange*).
   c. Set **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 that are available for Ad-hoc use on the associated RMX based on a needed bit rate for video.

d. In **Trunk Groups**, enter the administered SIP trunk groups you added in Procedure 5: Add a SIP Trunk Group for the Meeting Exchange System on page 125.

The Far End Resource Info, Resource Subscription, Priority Factory Number, and Standard Factory Number fields appear.

Figure 60: Example of the Video Bridge Form



e. Make sure **Far End Resource Info?** is set to **y**.

f. Set **Priority Factory Number** to the number you specified in the file conferenceProfile.cfg.

g. Set **Standard Factory Number**. to the number you specified in the file conferenceProfile.cfg.

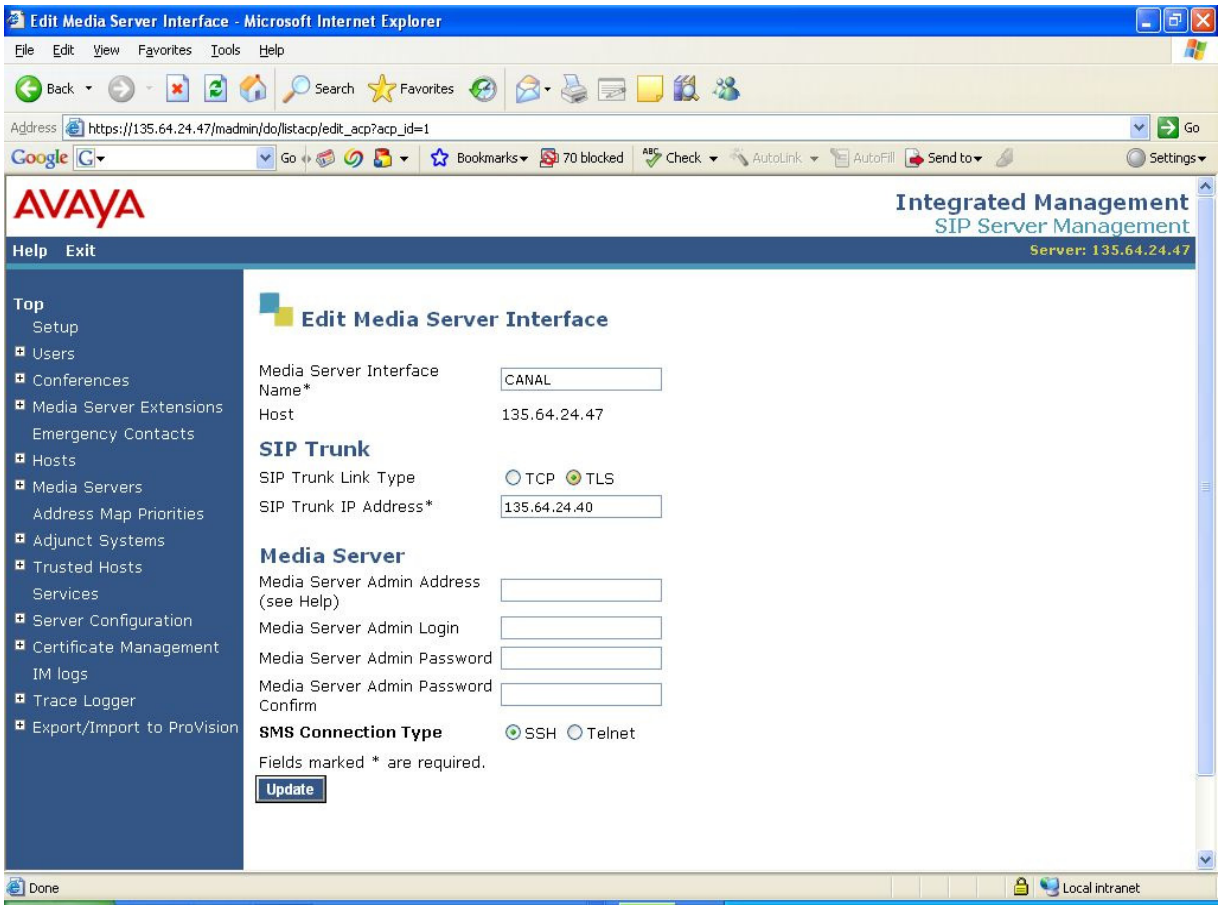
Procedure 9: Configure Avaya SES for Meeting Exchange 5.1 S6800

To configure Avaya SES for Meeting Exchange:

1. Log into the Avaya SES Administration interface (http://<ses-ipaddress>/admin) and verify that the SES is set up as a Home/Edge proxy. Other configurations are possible with multiple SES proxies. Select **Server Configuration>System Properties**, and verify that SIP Domain is set to the domain name administered on the Avaya Communication Manager signaling group.
2. For each SIP station, add a user on SES. (Select **Users>Add**.)
3. Add a media server interface. (Select **Media Server>Add**.) Be sure to set the following parameters:
   - **Media Server Interface Name** to the Avaya Communication Manager node name for its CLAN.
   - **SIP Trunk Line Type** to TLS.
   - **SIP Trunk IP Address** to the IP address of the CLAN interface.
   - **Media Server Admin Address** to the IP address to access SAT.
   - **Media Server Admin Login** to **init**.
   - **Media Server Admin Password** to the init password.
   - **Media Server Admin Password Confirm** to the init password.

   The following figures shows an example of the media server interface settings.

Figure 61: Example of the SES Media Server Interface Settings



4. Create a media server extension for each SIP user you added that will be configured as OPTIM. This informs SES to route all signaling calls from that user to the media server (Avaya Communication Manager). Select **Media Server Extensions>Add**. Be sure to set the following parameters:

   - **Extension** to the Avaya Communication Manager station to be associated with the user.
   - **Media Server** to the media server that you created.

   After creating the media server extension, map the media server extension to the user. (Select **Media Server Extensions>List Select <Assign> user ID** [the SIP user to map with this extension]).

   SES must understand where to route each number originating from a SIP endpoint and destined to a non-SIP endpoint or trunk.

5. Configure Avaya Meeting Exchange as a trusted host in SES. (Select **Trusted Hosts>Ad**d.) Set **IP Address** to the IP address of the Avaya Meeting Exchange system.

   Useful commands:

   trustedhost usage:

   trustedhost -L # list all third party trusted hosts currently configured

   trustedhost -a trusted-host-IP-address -n trusting-SES-IP-address [-c 'comment text'] # add new trusted host

   trustedhost -d trusted-host-IP-address -n trusting-SES-IP-address # delete a trusted host

   trustedhost -N # List all SES host IP addresses

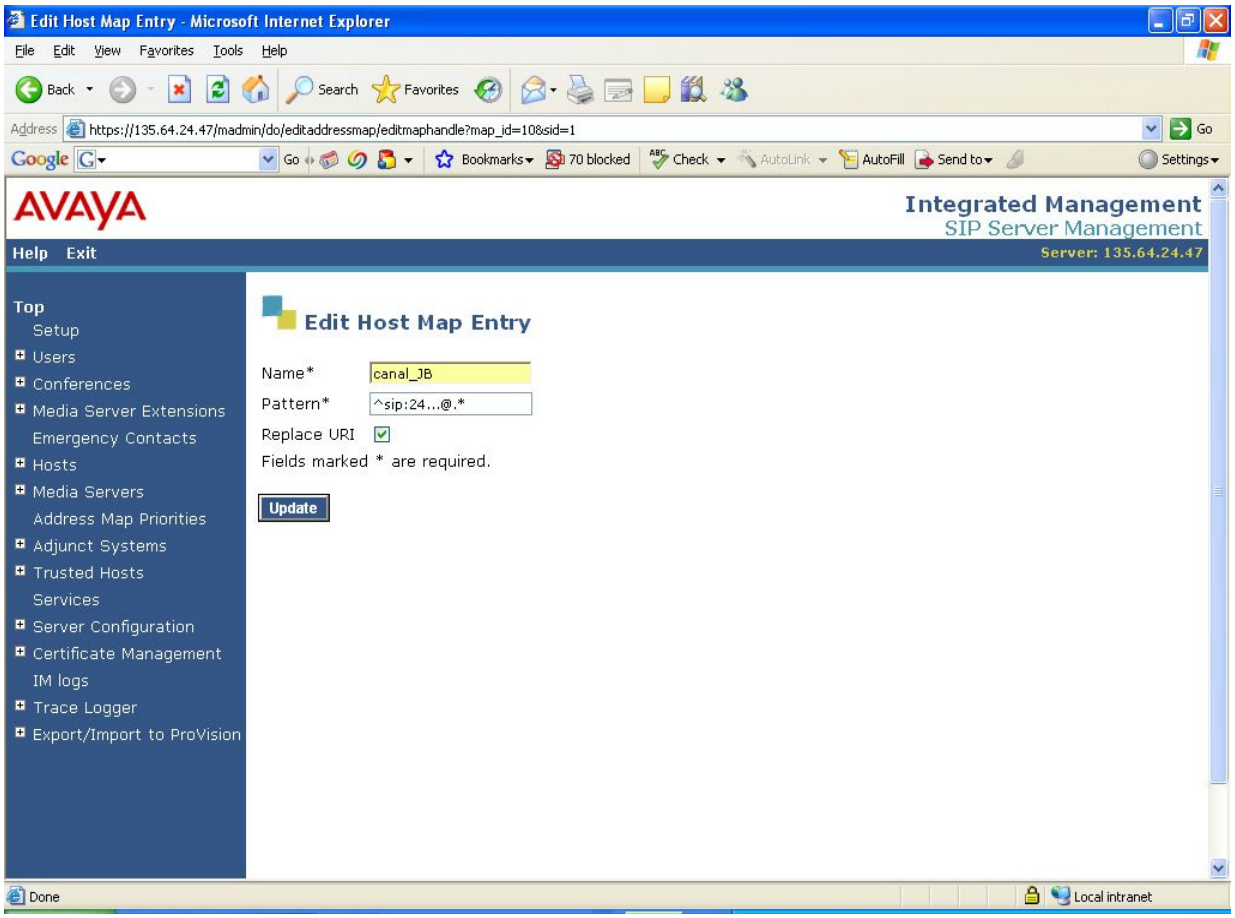
   trustedhost -V # -v can be used with any option

6. Configure SES to redirect calls to Avaya Meeting Exchange. (Select **Hosts>List Add Map in New Group**.) Set the following parameters:

   - Name to text that identifies the group.
   - Pattern to a regular expression to match SIP extensions.

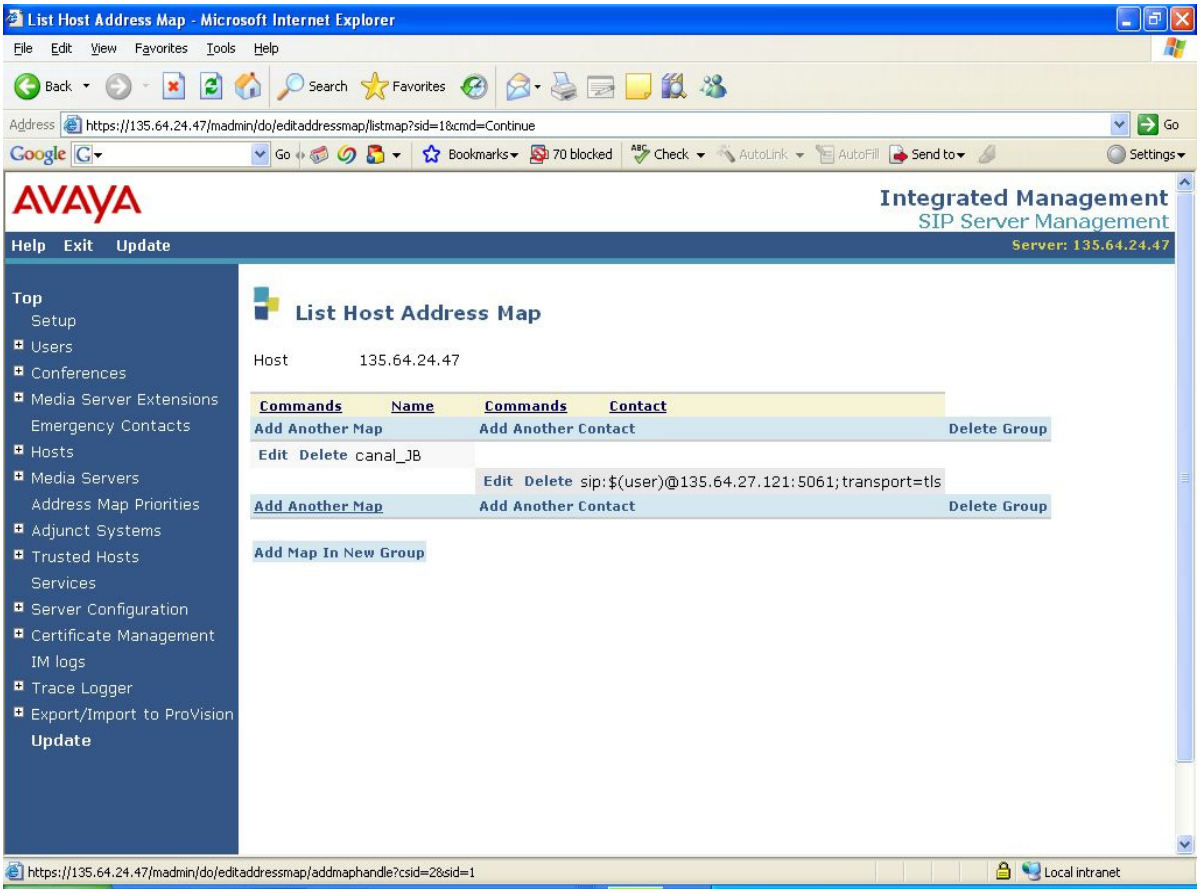
   The following figures shows an example of the Edit Host Map Entry page.

Figure 62: Example of the SES Edit Host Map Entry Page



After completing the Edit Host Map Entry page, click **Add another Contact** and set **Contact** to the SIP address for the Avaya Meeting Exchange system (for example, sip:$(user)@xxx.xxx.xxx.xxx:5060;transport=tls).

Figure 63: Example of the SES List Host Address Map Page



Configure a Polycom MGC Video Conferencing Bridge Platform as an H.320 Gateway

This section describes how to configure a Polycom MGC video conferencing bridge platform as an H.320 gateway.

Before performing the procedures in this section, make sure the MGC is already administered and registered to an Avaya Communication Manager system with inbound and outbound trunks correctly configured per the instructions in Configure Polycom MGC Video Conferencing Bridge Platforms with Avaya S8500 and S87xx Server on page 100.

Thing to Keep in Mind

Before configuring a Polycom MGC video conferencing bridge platform as an H.320 gateway, keep in mind the following information/recommendations:

- Use ARS for external H.320 calls.
- Use AAR for internal H.320 calls.
- Use external H.320 service prefixes (for example, 81=128 Kbps, 82=256 Kbps, 83=384 Kbps, 85=512 Kbps, etc.)
- Restrict video ISDN access appropriately (for example, via FRL/COR).
- Polycom MGC-25 systems and Polycom MGC 50/100 systems with one IP board should use the "single trunk group signaling group" administration.
- Polycom MGC 50/100 systems with multiple IP boards should change the "inbound trunk/signaling group" to an "inbound and gateway trunk/signaling group."

Trunk Groups

If the MGC is set up with outgoing and incoming trunk groups, you must create one incoming trunk group that may map to many signaling groups with one signaling group per IP board. This trunk group is the “incoming and gateway” trunk group.

Set the following parameters for the incoming and gateway trunk group:

- **Direction** to **two-way**.
- **Service Type** to **tie**.
- **Disconnect Supervision - In? t**o **y**.
- **Outgoing Display** to **y**.
- **Send Calling Number** to **y**.
- **Format** to **private**.

This incoming and gateway trunk group may consist of trunk members associated to many incoming and gateway ARQ+RRQ signaling groups. As result, the outgoing call traffic will spread across all signaling groups and IP boards.

Route Pattern

Use **add route-pattern xx** to create a new route pattern (a “Gateway Pattern”) per MGC Session Profile for H.323 to H.320 calls. The user will dial the dial plan prefix and the H.320/ H.323 number. The route pattern will omit the dial plan prefix and add the string **XXYY*** before the H.323/H.320 number, where **XXYY** is the IP service prefix and the Session Profile prefix, and ***** is the delimiter required by the gateway function.

Using AAR tables, enable the user to access the AAR table via a facility code and then an Avaya Communication Manager gateway prefix is created per MGC Session Profile. Use **change aar analysis** to add a dial string and map to the route pattern you created.

The Avaya Communication Manager system does not support dial strings that contain the ***** character or the **#** character as required by the MGC to support H.320 gateway functionality.

AAR Tables

Using AAR tables, the user accesses the AAR table via a facility code, and then an Avaya Communication Manager gateway prefix is created per MGC Session Profile. Use **change aar analysis** to add a dial string and map to the route pattern you created.

MGC Administration

On the MGC, perform the following steps:

1. On the H323 tab of the Network Service Properties dialog box, configure the following settings:
   - Set **Use Gatekeeper** to **Specify**.
   - Set **Preferred Gatekeeper IP Address or Name** to the IP address of the CLAN for the Avaya Communication Manager system to which you want this MGC system to register.
   - Set **Service Mode** to **Pseudo Gatekeeper - AVF**. (This setting will trigger H.225 (RAS) negotiation of the Avaya Video feature.)
   - Enable the **Refresh H.323 Registrations Every** check box, and enter **40** in the associated box. (Setting the refresh to 40 seconds will help prevent signaling group dop outs.)
2. Under **Network Services>ISDN**, create the required ISDN service. Configure the following settings in the Network Service Properties dialog box:
   - On the Settings tab, set **Span Type** to **E1** or **T1**.
   - On the PRI Settings tab, set **Default num-type** to **Unknown** if you want the network to interpret the dialing digits for routing the call.

- On the Span Definition tab:
  - Set **Framing** to the frame format used by the carrier.
  - Set Line Coding to the appropriate setting for E1 or T1.
  - Set Switch Type to the appropriate setting for E1 or T1.
- On the Spans and Phones tab:
  - In the Spans list box, enter an identity (Circ. Id) for this service.
  - In the Dial In Phone Num list box, enter the range of dial-in phone numbers allocated to the MCU function by the service provider. You can specify several ranges for a span.
  - In the MCU Number box, enter the MCU dial-out identity.
  - In the Gateway Range list box, enter the range of dial-in numbers allocated to gateway calls. The range of dial-in numbers allocated to gateway calls must differ from the dial-in number ranges allocated to MCU function.

3. Configure the network interface module in conjunction with the ISDN network services defined in the MGC Manager to connect the MCU to the ISDN network. (Set **circ.id**, and set the primary clock source.)
4. For the network card, enter the circuit ID specified in the ISDN network service.
5. Partition and assign DID numbers to the MGC interface. For assigned DID numbers, ensure:
   - UDP, AAR, and route pattern are administered to route PRI DIDs to the PRI trunk group/ signaling group/DS1 of the MGC.
   - the MGC's gateway number ranges and MCU number ranges are assigned and match the Avaya Communication Manager administration.
6. Under **Gateway Configuration>Session Profiles>To H.320 Session Profil**e, create a profile with the matching E.164 as per the AAR table and route pattern, and assign an ISDN service. Ensure Transcoding is set to always.
7. Under **Gateway Configuration>Session Profiles>To H.323 Session Profile**, create a profile and assign the IP service that corresponds to an IP board/CLAN. Ensure Transcoding is set to always.
8. Change the delimiter to ***** instead of **#** or vice versa (that is, consistent administration between the route pattern and the MGC expected delimiter).

Configure a SE200 Gatekeeper

This section describes how to configure a SE200 Gatekeeper.

Checklist

When setting up these systems, you will need to know the following information:

- the IP codec sets you want to use
- the IP network regions you want use
- the IP address of the IP board for the gatekeeper

Configuration Procedures

To configure a SE200 gatekeeper, you must perform the following steps:

1. Add an entry in the IP Node Names for the SE200.
2. Add a signaling group for the SE200.
3. Add a trunk group for the SE200.
4. Modify the signaling group for the SE200.
5. Create a route pattern to the SE200.
6. Configure the SE200.

Procedure 1: Add an Entry in the IP Node Names for the SE200

To add an entry in the IP Node Names form for the SE200 system:

1. Use the **change node-names ip** command to access the IP Node Names form.
2. In the Name field, enter a name for the SE200 system.
3. In the corresponding IP Address field, enter the IP address of the IP board for the SE200 system.

Procedure 2: Add a Signaling Group for the SE200

To add a signaling group for the SE200 system:

1. Use the **add signaling-group *xx*** command (where ***xx*** is the chosen signaling group) to access the Signaling Group form.

   The Signaling Group form appears.

2. Set **Group Type** to **h.323**.
3. Set **IP Video** to **y**.
4. Set **Priority Video**. If you want all incoming calls to receive priority video transmissions, select **y**.
5. Set **Near-end Listen Port** to **1719**.
6. Set **LRQ Required** to **y**.
7. Set **Far-end Node Name** to the name you entered for the SE200 system.
8. Set **Far-end Listen Port** to **1719**.
9. Set the **Far-end Network Region** to the appropriate IP network region.
10. Set **Direct IP-IP Audio Connections** to **y**.
11. Set **IP Audio Hairpinning** to **y**.

Procedure 3: Add a Trunk Group for the SE200

To add a trunk group for the SE200 system:

1. Use the **add trunk-group *xx*** command (where ***xx*** is the chosen trunk group) to access the Trunk Group form.

   The Trunk Group form appears.

2. Set **Group Type** to **isdn**.
3. Set **Carrier Medium** to **IP**.
4. Go to page 5 of the Trunk Group form.
5. Add members to the trunk group.

Procedure 4: Modify the Signaling Group

To modify the signaling group for the SE200 system:

1. Use the **change signaling-group *xx*** command (where ***xx*** is the signaling group you added) to access the Signaling Group form.

   The Signaling Group form appears.

2. Set **Trunk Group for Channel Selection** to the trunk group you just added.

Procedure 5: Create a Route Pattern for the SE200

To create a route pattern that points to the trunk group:

1. Use the **change route-pattern *xx*** command (where ***xx*** is the route pattern you want to use) to access the Route Pattern form.

   The Route Pattern form appears.

2. In the **Grp No** field, enter the number of the trunk group you created for the SE200.

Procedure 6: Configure the SE200

Follow the instructions provided with the system to install and configure the SE200 gatekeeper.

SE200 Limitations

Question 1: Will you be attempting to use an audio-only endpoint to transfer an SE200 device into a video call?

☐ **Yes**. Expect audio-only calls. Once an SE200 has become part of an audio call, it will not regain video without hanging up and starting again. Avoid this by dialing the SE200 endpoint directly into the call, or using a video-capable endpoint to conduct the transfer.

☐ **No**.

Question 2: Will you be attempting to transfer calls from a trunked SIP video device to an SE200 device?

☐ **Yes**. Expect some audio-only calls. Unless this transfer is completed quickly, before video comes up between the transferring device and the SE200, the eventual call will not get video. The SE200 is not able to complete the required call setup steps to make this scenario reliable.

☐ **No**.

Question 3: Have you disabled shuffling in the SE200's network region?

☐ **Yes**.

☐ **No**. Expect some call failures in transfer scenarios. The SE200 is not able to complete the required call setup steps to make this scenario reliable.

Configure a Tandberg Centric 1700 MXP

This section describes how to configure the Tandberg Centric 1700 MXP. It contains two sections, as follows:

- Configure H.323 Stations to Support a Tandberg Centric 1700 MXP
- Configure a Tandberg Centric 1700 MXP

Tip:

In addition, Tandberg Endpoint Limitations on page 160 describes a number of limitations associated with Tandberg endpoints.

Configure H.323 Stations to Support a Tandberg Centric 1700 MXP

This section describes how to configure H.323 stations on Avaya Communication Manager to support the Tandberg Centric 1700 MXP. Each Tandberg Centric 1700 MXP requires four stations on Avaya Communication Manager. Repeat these steps for each Tandberg Centric 1700 MXP in your network.

1. Issue the command **`add station <n>`**, where **`n`** is the extension of an available station and configure as follows:

Figure 64: Add Station Command

```
add station 33621                                    Page 1 of 4
                              STATION
Extension: 33621                 Lock Messages? n      BCC: 0
Type: H.323                      Security Code: 123456 TN: 1
Port: IP                         Coverage Path 1:      COR: 1
Name: Tandberg1700               Coverage Path 2:      COS: 1
                                 Hunt-to Station: Tests? y
STATION OPTIONS
                                 Time of Day Lock Table:
   Loss Group: 19            Message Waiting Indicator: none
                             Authentication Required? y
   Survivable COR: internal
   Survivable Trunk Dest? y
   DTMF over IP: in-band
                                                IP Video? y
```

2. Repeat step 1 to add a second, third, and fourth station for the Tandberg Centric 1700 MXP.
3. Issue the command **change station <n>**, where **n** is the extension of an available station and configure as follows:

   Note:

   Set the **Hunt-to-Station** field to the extension of the second station configured for the Tandberg Centric 1700 MXP.

Figure 65: Change Station Command

```
change station 33621                                  Page 1 of 4
                              STATION
Extension: 33621                 Lock Messages? n      BCC: 0
Type: H.323                      Security Code: 123456 TN: 1
Port: IP                         Coverage Path 1:      COR: 1
Name: Tandberg1700               Coverage Path 2:      COS: 1
                                 Hunt-to Station: 33622 Tests? y
STATION OPTIONS
                                 Time of Day Lock Table:
Loss Group: 19                   Message Waiting Indicator: none
                                 Authentication Required? y
   Survivable COR: internal
   Survivable Trunk Dest? y
   DTMF over IP: in-band
                                                 IP Video? y
```

4. Repeat step 3 to configure the second, third, and fourth station for the Tandberg Centric 1700 MXP.

Note:

For the second station, set the **Hunt-to-Station** field to the extension of the third station configured for the Tandberg Centric 1700 MXP. For the third station, set the the **Hunt-to-Station** field to the extension of the fourth station configured for the Tandberg Centric 1700 MXP. For the fourth station, set the the **Hunt-to-Station** field to the extension of the first station configured for the Tandberg Centric 1700 MXP.

Configure a Tandberg Centric 1700 MXP

Note:

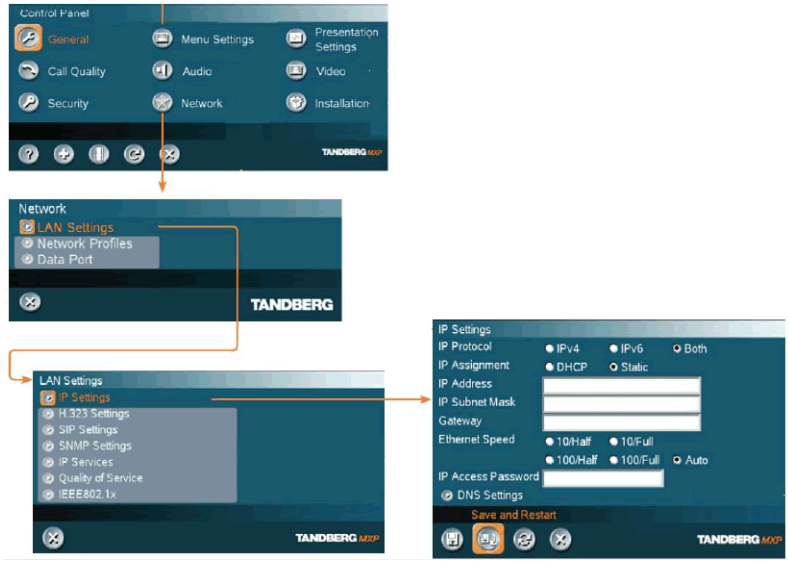
The Tandberg endpoints do not support Dynamic Host Conifguration Protocol (DHCP) Option 242. This option is required in a network if there are Avaya 9600 Series Telephones present and DHCP is utilized. The workaround is to statically configure the H.323 gatekeeper on the Tandberg endpoints.

You must configure Tandberg endpoints using the Control Panel Menus or the Command Line Interface (CLI). If you are configuring the H.323 gatekeeper on the Tandberg endpoints, you must also use the Control Panel Menus or CLI.

In the example in this guide, DHCP is disabled. Information regarding IP addressing was entered statically using the Control Panel Menus. Static IP addressing simplifies the assignment of Tandberg endpoints to the correct IP network region. You can access the Control Panel Menus as follows:

1. On the Tandberg Centric 1700 MXP remote control unit, navigate to **Network** > **LAN Settings** > **IP Settings**. For more information, see Figure 66.

Figure 66: Tandberg Centric 1700 MXP remote control unit



2. On the **IP Settings** panel, select **Static** IP Assignment and enter the IP details in the various fields on the panel.

   Note:

   On this panel, the **IP Access Password** field refers to the password used to access the Tandberg endpoint using the CLI. You can change the IP Access Password here.

To configure the Tandberg Centric 1700 MXP:

1. Log in to the Tandberg Centrix 1700 MXP using Secure Shell (SSH).
2. At the command line, enter the following commands.

   Note:

   You must enter commands that begin with xConfiguration H323Gatekeeper at the command line. You can, if you wish, enter the other commands using the Control Panel Menus on the Tandberg Centric 1700 MXP.

Figure 67: Configuration Commands

```
xConfiguration H323 Mode: On
xConfiguration H323CallSetup Mode: Gatekeeper
xConfiguration H323Prefix: ""
xConfiguration H323Gatekeeper Discovery: Manual
xConfiguration H323Gatekeeper Address: <IP Address of CLAN>
xConfiguration H323Gatekeeper Authentication Mode: Off
xConfiguration H323Gatekeeper Authentication ID: ""
xConfiguration H323Gatekeeper MultipleAlias: Off
xConfiguration H323Gatekeeper Avaya Mode: On
xConfiguration H323Gatekeeper Avaya AnnexH: On
xConfiguration H323Gatekeeper Avaya MultipointCount: 0
xconfiguration H323Gatekeeper Avaya Password: <Security Code from
  Step 1 in Configure H.323 Stations to Support a Tandberg Centric
  1700 MXP on page 152>
xConfiguration Conference H323Alias E164: <Station Extension from
  Step 1 in Configure H.323 Stations to Support a Tandberg Centric
  1700 MXP on page 152>
xConfiguration Conference H323Alias ID: ""
```

3. To apply these changes, request a boot:

```
boot


OK
Boot requested, restarting
```

Configure a Tandberg Centric 150 MXP

This section describes how to configure the Tandberg Centric 150 MXP. It contains two configuration sections, as follows:

- Configure H.323 Stations to Support a Tandberg Centric 150 MXP
- Configure a Tandberg Centric 150 MXP

This section also describes a number of the current limitations associated with Tandberg endpoints:

- Tandberg Endpoint Limitations

Configure H.323 Stations to Support a Tandberg Centric 150 MXP

This section describes how to configure an H.323 stations on Avaya Communication Manager to support the Tandberg Centric 150 MXP.

1. Issue the command **add station <n>**, where **n** is the extension of an available station and configure as follows:

   Note:

   Repeat step 1 for each Tandberg Centric 150 MXP in the network.

Figure 68: Add Station Command

```
add station 33611                                Page 1 of 4
                                    STATION
Extension: 33611                    Lock Messages?   n     BCC: 0
Type: H.323                         Security Code: 123456 TN: 1
Port: IP                            Coverage Path 1:      COR: 1
Name: Tandberg150                   Coverage Path 2:      COS: 1
                                    Hunt-to Station: Tests? y
STATION OPTIONS
                                    Time of Day Lock Table:
         Loss Group: 19             Message Waiting Indicator: none
                                    Authentication Required? y
Survivable COR: internal
Survivable Trunk Dest? y
DTMF over IP: in-band
                                                 IP Video? y
```

2. Optionally, you can repeat step 1 to add a second station for the Tandberg Centric 150 MXP. This second station is used to support a second calling line and is an optional step. The Tandberg Centric 150 MXP supports a maximum of two calling lines. If you perform this step, you must perform step 3.

3. Issue the command **change station <n>**, where **n** is the extension of the first station that you configured for the Tandberg Centric 150 MXP and configure as follows:

   Note:

   Set the **Hunt-to-Station** field to the extension of the second station configured for the Tandberg Centric 150 MXP. Since there are only two stations used to support the Tandberg Centric 150 MXP, you only need to administer hunting from the first station to the second station. You do not have to administer the second station to hunt back to the first station. If more than two stations are used, you must complete the loop and administer the last station to hunt to the first station, as for the Tandberg Centric 1700 MXP.

Figure 69: Change Station Command

```
change station 33611                                  Page 1 of 4
                                   STATION
Extension: 33611                   Lock Messages? n       BCC: 0
Type: H.323                        Security Code: 123456  TN: 1
Port: IP                           Coverage Path 1:       COR: 1
Name: Tandberg150                  Coverage Path 2:       COS: 1
                                   Hunt-to Station: 33612 Tests? y
STATION OPTIONS
                                   Time of Day Lock Table:
Loss Group: 19                     Message Waiting Indicator: none
                                   Authentication Required? y
Survivable COR: internal
Survivable Trunk Dest? y
DTMF over IP: in-band
                                                  IP Video? y
```

Configure a Tandberg Centric 150 MXP

This section describes how to configure the Tandberg Centric 150 MXP. Figure 70 shows the Tandberg keypad. You can use the Tandberg Centric 150 MXP keypad to access the Control Panel Menus. You can access the Control Panel Menus as follows:

1. On the Tandberg Centric 150 MXP remote control unit, navigate to **Network** > **LAN Settings** > **IP Settings**.

2. On the **IP Settings** panel, select **Static** IP Assignment and enter the IP details in the various fields on the panel.

Figure 70: Tandberg Keypad

To configure the Tandberg Centric 150 MXP:

1. Log in to the Tandberg Centrix 150 MXP using Secure Shell (SSH).
2. At the command line, enter the following commands:

Note:

You must enter commands that begin with xConfiguration H323Gatekeeper at the command line. You can, if you wish, enter the other commands using the Control Panel Menus on the Tandberg Centric 150 MXP. Also, please note that to enable multiple line appearances for the Tandberg Centrix 150 MXP, set the variable for **`xConfiguration H323Gatekeeper Avaya MultipointCount`** to **`2`**.

Figure 71: Configuration Commands

```
xConfiguration H323CallSetup Mode: Gatekeeper
xConfiguration H323Gatekeeper Discovery: Manual
xConfiguration H323Gatekeeper Address: <IP Address of CLAN>
xConfiguration H323Gatekeeper Authentication Mode: Off
xConfiguration H323Gatekeeper Authentication ID: ""
xConfiguration H323Gatekeeper MultipleAlias: Off
xConfiguration H323Gatekeeper Avaya Mode: On
xConfiguration H323Gatekeeper Avaya AnnexH: On
xConfiguration H323Gatekeeper Avaya MultipointCount: 2
xconfiguration H323Gatekeeper Avaya Password: <Security Code from
  Step 1 in Configure H.323 Stations to Support a Tandberg Centric
  150 MXP on page 157>
xConfiguration Conference H323Alias E164: <Station Extension from
  Step 1 in Configure H.323 Stations to Support a Tandberg Centric
  150 MXP on page 157>
xConfiguration Conference H323Alias ID: ""
```

3. To apply these changes, request a boot:

```
boot


OK
Boot requested, restarting
```

Tandberg Endpoint Limitations

In the current release, there are a number of limitations associated with Tandberg endpoints.

- The Tandberg endpoint may not shuffle correctly. Typically, this issue results in a call with video but without audio, or the call may drop completely. The workaround is to place Tandberg endpoints into a non-shuffling region.
- The video and/or the audio quality to and from the Tandberg endpoint may fall below expectations. Currently, there is no known workaround. The issue is caused by the incorrect ordering of video caps.
- In a multipoint call, it may not be possible to answer an incoming call for a third Participant. The current workaround is to dial in the reverse direction.

Configure Unauthenticated H.323 Endpoints

From Communication Manager 4.1 onwards, the Avaya Video Telephony Solution supports legacy non-AVTS H.323 video endpoints in single point mode for basic call establishment. This section describes how to configure the system to enable unauthenticated H.323 support. It contains the following sections:

- Enabling Licensing
- Administering the Station
- Configuring Third Party Pause

Enabling Licensing

To enable licensing for unauthenticated H.323 support, you must obtain a new RFA license.

The form **system-parameters customer-options** contains the following relevant licensing counts:

Max Concur Registered Unauthenticated H.323 Stations

Maximum Video Capable H.323 Stations

The form **change system-parameters special applications** contains the following relevant option feature:

(SA8697) - 3rd Party H.323 Endpoint Support?

Administering the Station

When you add the station, ensure that:

- **Type** is **H.323**
- **Authentication Required?** is **n**
- **IP Video** is **y**
- **Security Code** is clear

Figure 72 shows an example.

Figure 72: Example of an H.323 Add Station

```
add station 71842                              Page   1 of   4
                                             STATION
Extension: 71842                  Lock Messages? n       BCC: 0
     Type: H.323                  Security Code:         TN: 1
     Port: IP                     Coverage Path 1:       COR: 1
     Name: Unauthenticated 1      Coverage Path 2:       COS: 1
                                  Hunt-to Station:       Tests? y
STATION OPTIONS
                                  Time of Day Lock Table:
          Loss Group: 19          Message Waiting Indicator: none
                                  Authentication Required? n
   Survivable COR: internal
   Survivable Trunk Dest? y
   DTMF over IP: in-band
                                  IP Video? y
```

Configuring Third Party Pause

Third party pause allows audio to shuffle during a video call to a legacy endpoint, but to do so requires video to be temporarily disconnected. Enabling third party pause for a legacy/ unauthenticated endpoint may cause undesirable effects such as loss of audio, video or dropped calls. Many legacy video endpoints do not support third party pause signaling (TCS=0). Avaya has devised a workaround, as follows:

1. Create a network region for use with those endpoints.
2. Disable audio shuffling as follows:

Figure 73: Disabled Audio Shuffling

```
change ip-network-region 6                     Page   1 of  19
                                IP NETWORK REGION
  Region: 6
Location:           Authoritative Domain:
    Name: Non-shuffling
MEDIA PARAMETERS               Intra-region IP-IP Direct Audio: no
   Codec Set: 4                Inter-region IP-IP Direct Audio: no
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 3029
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): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

3. Ensure that inter region connectivity is configured appropriate, for example:

Figure 74: Example of Inter Region Connectivity

```
change ip-network-region 6                          Page   3 of  19
                Inter Network Region Connection Management
src      dst   codec direct     WAN-BW-limits    Video      Dyn
rgn rgn  setWAN Units Total  NormPrioShrIntervening-regions  CAC IGAR
 6   1    2      y    NoLimit                                  n
 6   2
 6   3
 6   4
 6   5
 6   6    0
 6   7    4      y    NoLimit                                  n
 6   8
 6   9
 6   10
 6   11
 6   12
 6   13
 6   14
 6   15
```

4. Use the **ip-network-map** to assign individual IP adddresses or address ranges to the non-shuffling network region.

   Note:

   The station is expected not to change IP addresses.

   Either use static addressing on the endpoint or map the MAC address on the DNS to a single IP address. Figure 75 shows an example.

Figure 75: Example IP Network Map

```
change ip-network-map                                    Page   1 of  32
                          IP ADDRESS MAPPING
                                                                 Emergency
                                                Subnet            Location
From IP Address(To IP Address   or Mask)  Region    VLAN   Extension
 135.8  .63 .1    135.8  .63 .254         6          n
 135.27 .66 .1    135.27 .66 .99          6          n
 135.27 .66 .100  135.27 .66 .100         6          n
 135.27 .66 .209  135.27 .66 .209         1          n
 135.27 .66 .232  135.27 .66 .232         2          n
 135.27 .67 .21   135.27 .67 .21          2          n
 135.27 .67 .29   135.27 .67 .29          1          n
 135.27 .67 .47   135.27 .67 .47          2          n
```

Configure a Direct Routing Gatekeeper

This section describes how to configure a direct routing gatekeeper.

Thing to Keep in Mind

Before configuring a direct routing gatekeeper, keep in mind the following information/ recommendations:

- Avaya Communication Manager to direct gatekeeper calls should use an “outbound” route pattern, ISDN tie trunk group, and H.323 LRQ signaling group.
- Direct gatekeeper to Avaya Communication Manager calls should use a second “incoming” ISDN tie trunk group and either a single “incoming” H.323 signaling group with far-end unspecified or many “incoming-per-ept” H.323 signaling groups.
- Dial plan analysis, UDP, and AAR analysis should route the direct gatekeeper extension range to the “outbound” trunk group.
- Direct gatekeeper inter-gatekeeper LRQ administration for extensions managed by Avaya Communication Manager.

Checklist

When setting up these systems, you will need to know the following information:

- the IP codec sets you want to use
- the IP network regions you want use
- the IP address of the IP board for the gatekeeper

Configuration Procedures

To configure a direct gatekeeper, you must perform the following steps:

1. Add an entry in the IP Node Names for the direct gatekeeper.
2. Add an outbound signaling group for the direct gatekeeper.
3. Add an outbound trunk group for the direct gatekeeper.
4. Modify the outbound signaling group for the direct gatekeeper.
5. Create a route pattern to the direct gatekeeper.

6. Add an inbound signaling group for the direct gatekeeper.
7. Add an inbound trunk group for the direct gatekeeper.
8. Modify the inbound signaling group for the direct gatekeeper.
9. Add an H.323 video signaling group per endpoint managed by the direct gatekeeper.
10. Modify the inbound trunk group.
11. Configure the direct gatekeeper.

Procedure 1: Add an Entry in the IP Node Names for the Gatekeeper

To add an entry in the IP Node Names form for the gatekeeper:

1. Use the **change node-names ip** command to access the IP Node Names form.
2. In the Name field, enter a name for the system.
3. In the corresponding IP Address field, enter the IP address of the IP board for the system.

Procedure 2: Add an Outbound Signaling Group for the Gatekeeper

To add an outbound signaling group for the system:

1. Use the **add signaling-group *xx*** command (where ***xx*** is the chosen signaling group) to access the Signaling Group form.

   The Signaling Group form appears.
2. Set **Group Type** to **h.323**.
3. Set **IP Video** to **y**.
4. Set **Priority Video**. If you want all incoming calls to receive priority video transmissions, select **y**.
5. Set **Near-end Listen Port** to **1719**.
6. Set **LRQ Required** to **n**.
7. Set **RRQ Required** to **n**.
8. Set **Far-end Node Name** to the name you entered for the system.
9. Set **Far-end Listen Port** to **1719**.
10. Set the **Far-end Network Region** to the appropriate IP network region.
11. Set **Direct IP-IP Audio Connections** to **y**.
12. Set **IP Audio Hairpinning** to **n**.

Procedure 3: Add an Outbound Trunk Group for the Gatekeeper

To add an outbound trunk group for the system:

1. Use the **add trunk-group *xx*** command (where ***xx*** is the chosen trunk group) to access the Trunk Group form.

   The Trunk Group form appears.

2. Set **Group Type** to **isdn**.
3. Set **Carrier Medium** to **IP**.
4. Go to page 5 of the Trunk Group form.
5. Add members to the trunk group.

Procedure 4: Modify the Outbound Signaling Group

To modify the outbound signaling group for the system:

1. Use the **change signaling-group *xx*** command (where ***xx*** is the signaling group you added) to access the Signaling Group form.

   The Signaling Group form appears.

2. Set **Trunk Group for Channel Selection** to the trunk group you just added.

Procedure 5: Create a Route Pattern for the Gatekeeper

To create a route pattern that points to the trunk group:

1. Use the **change route-pattern *xx*** command (where ***xx*** is the route pattern you want to use) to access the Route Pattern form.

   The Route Pattern form appears.

2. In the **Grp No** field, enter the number of the trunk group you created for the system.

Procedure 6: Add an Inbound Signaling Group for the Gatekeeper

To add an inbound signaling group for the system:

1. Use the **add signaling-group *xx*** command (where ***xx*** is the chosen signaling group) to access the Signaling Group form.

   The Signaling Group form appears.

2. Set **Group Type** to **h.323**.
3. Set **IP Video** to **y**.
4. Set **Priority Video**. If you want all incoming calls to receive priority video transmissions, select **y**.

5. Set **Near-end Listen Port** to **1720**.
6. Set **LRQ Required** to **n**.
7. Set **RRQ Required** to **n**.
8. Set the **Far-end Network Region** to the appropriate IP network region.
9. Set **Direct IP-IP Audio Connections** to **y**.
10. Set **IP Audio Hairpinning** to **n**.

Procedure 7: Add an Inbound Trunk Group for the Gatekeeper

To add an inbound trunk group for the system:

1. Use the **add trunk-group *xx*** command (where ***xx*** is the chosen trunk group) to access the Trunk Group form.

   The Trunk Group form appears.
2. Set **Group Type** to **isdn**.
3. Set **Carrier Medium** to **IP**.
4. Go to page 5 of the Trunk Group form.
5. Add members to the trunk group.

Procedure 8: Modify the Inbound Signaling Group

To modify the signaling group for the system:

1. Use the **change signaling-group *xx*** command (where ***xx*** is the signaling group you added in Procedure 6) to access the Signaling Group form.

   The Signaling Group form appears.
2. Set **Trunk Group for Channel Selection** to the trunk group you just added.

Procedure 9: Add an H.323 Video Signaling Group

Perform the following steps to add an H.323 video signaling group per endpoint managed by the direct gatekeeper:

1. Use the **add signaling-group *xx*** command (where ***xx*** is the chosen signaling group) to access the Signaling Group form.

   The Signaling Group form appears.
2. Set **Group Type** to **h.323**.
3. Set **LRQ Required** to **n**.
4. Set **RRQ Required** to **n**.

5. For endpoints that do not support “third-party pause,” place the signaling group in an IP network region with direct-ip inter-region disabled.

Procedure 10: Modify the Inbound Trunk Group

Modify the “inbound” trunk group to include one trunk member per endpoint managed by the direct gatekeeper.

Procedure 11: Configure the Gatekeeper

Follow the instructions provided with the system to install and configure the gatekeeper.

Configure Video Trunks between Two Avaya Communication Manager Systems

This section describes how to configure video trunks between two Avaya Communication Manager systems.

Checklist

When setting up these video trunks, you will need to know the following information:

- the IP address of the CLAN or PCLAN of the other Avaya Communication Manager system
- the IP network regions you want use

Configuration Procedures

To configure a video trunk between two Avaya Communication Manager systems, you must perform the following steps:

1. Add an entry in the IP Node Names for the video trunk.
2. Add a signaling group for the trunk.
3. Add the trunk.
4. Modify the signaling group.
5. Create a route pattern for the trunk.

Procedure 1: Add an Entry in the IP Node Names for the Video Trunk

To add an entry in the IP Node Names form for the video trunk:

1. Use the **change node-names ip** command to access the IP Node Names form.
2. In the Name field, enter a name for the video trunk.
3. In the corresponding IP Address field, enter the IP address of the CLAN or PCLAN of the other Avaya Communication Manager system.

Procedure 2: Add a Signaling Group for the Video Trunk

To add a signaling group for the video trunk:

1. Use the **add signaling-group *xx*** command (where ***xx*** is the chosen signaling group) to access the Signaling Group form.

   The Signaling Group form appears.

2. Set **Group Type** to **h.323**.
3. Set **IP Video** to **y**.
4. Set **Near-end Listen Port**.
5. Set **LRQ Required** to **n**.
6. Set **Far-end Node Name**.
7. Set **Far-end Listen Port**.
8. Set the **Far-end Network Region**. If you set the maximum bandwidth for video calls in Procedure 3, assign that IP network region.
9. Set **Calls Share IP Signaling Connection** to **y**.

   Note:

   You must set this parameter to **y**.

10. Set **Direct IP-IP Audio Connections** to **y**.
11. Set **IP Audio Hairpinning** to **y**.

Procedure 3: Add a Trunk Group

To add a trunk group:

1. Use the **add trunk-group *xx*** command (where ***xx*** is the chosen trunk group) to access the Trunk Group form.

   The Trunk Group form appears.

2. Set **Group Type** to **isdn**.
3. Perform one of the following steps:
   - For Avaya Communication Manager Release 3.01, set **Carrier Medium** to **IP**.
   - For Avaya Communication Manager Release 3.1 or later, set **Carrier Medium** to **H.323**.
4. Go to page 5 of the Trunk Group form.
5. Add members to the trunk group.

Procedure 4: Modify the Signaling Group

To modify the signaling group video trunk:

1. Use the **change signaling-group *xx*** command (where ***xx*** is the signaling group you added) to access the Signaling Group form.

   The Signaling Group form appears.

2. Set **Trunk Group for Channel Selection** to the trunk group you just added.

Procedure 5: Create a Route Pattern for the Video Trunk

To create a route pattern that points to the trunk group:

1. Use the **change route-pattern *xx*** command (where ***xx*** is the route pattern you want to use) to access the Route Pattern form.

   The Route Pattern form appears.

2. In the **Grp No** field, enter the number of the trunk group you created.

Monitor the Status of Video Bandwidth Usage

This procedure describes how to monitor the status of video bandwidth usage for inter-network regions.

Use the **status ip-network-region *x*** command (where ***x*** is the chosen IP network region) to view the video bandwidth usage. The current video bandwidth usage to each network region is displayed.

Use the **change ip-network-region *x*** command (where ***x*** is the chosen IP network region) to specify the maximum amount of bandwidth that can be used for video to each IP network region.

Communication Manager Selection of Video Bridge

Note:

Ad-hoc conferences are conferences that Users create to instantly address a specific temporary requirement to converse. Ad-hoc conferences are unscheduled and generally unplanned.

For ad-hoc video conference hosting in a multiple bridge configuration, Communication Manager uses logic to select the least loaded bridge. It will firstly consider bandwidth limitations between network regions, looking for the bridge that will provide video connectivity to the most endpoints, and provide audio to all. It will then look at available resources on the bridge, considering number of ports available and number of conferences that can be hosted. Communication Manager considers port and conference availability as a percentage of overall capacity. In a configuration with two equally accessible bridges, if one bridge has 90% availability and the other has 100% availability, Communication Manager hosts the ad-hoc video conference on the bridge that has 100% availability. If two bridges have identical percentage availability, Communication Manager hosts the ad-hoc video conference on the lowest numbered bridge.

Communication Manager will not use a bridge that cannot provide video to at least two of the endpoints and will not use a bridge that cannot provide audio to all of the endpoints. If no bridges meet the criteria, Communication Manager will continue audio-only.

To view live information in relation to availability for ad-hoc video conferences:

1. On each Communication Manager server with a video endpoint, open a PuTTY session (or connect directly to SAT with ASA or similar).

2. Log in to SAT and at the SAT command line, enter the following command:

   `list video-bridge`

   This will list configured bridges. On Communication Manager 5.2 or later, this will also show service status, network region, and bridge type.

3. For each bridge of interest, enter the command:

   `status video-bridge xx`

   This will show bridge status, port and conference usage, capacity, and some historical information.

Ad-hoc Licensing Considerations

Customers can buy licenses from Avaya to enable their ports to function as ad-hoc video conferencing ports.

Note:

The offer code for the Communication Manager (CM) Remote Feature Activation (RFA) license file is 224020. This code enables a single port to function as an ad-hoc video conferencing port at a nominal cost of one cent per port.

To determine how many ad-hoc video conferencing ports that you require in your organization, you must consider a number of points:

- You should consider the number of Users to whom you intend to allocate the ad-hoc video conferencing capability. Using the Class of Service (COS) setting, you can control the allocation of this feature to individual stations. For more information about COS, see Procedure 2: Configure Class of Service on page 60.
- You should also consider the bandwidth usage patterns of each station. A typical Avaya IP Softphone User consumes 384 KBps, which equates to a single port. However, using a COS level with Priority Video Calling, you can choose to allocate a higher bandwidth, such as 768 KBps, to selected VIP Users. These Users will each now occupy multiple ports. For more information about COS, see Classifying Video Users on page 9.
- You should consider the transmission medium; IP or ISDN. IP (H.323) is usually achieved using the Customer LAN, WAN, or Internet. ISDN (H.320) can involve a direct connection to a Local Exchange Carrier (LEC) or a long distance vendor or a connection to a Communication Manager product.
- You should consider whether you intend to isolate a certain number of ports for selected VIP Users. In this scenario, you can segregate a number of ports to ensure guaranteed port availability even during high usage peak times. This configuration limits port availability for regular Users.

- Lastly, before making a decision on the number of ad-hoc video conferencing ports that you require, it is a good idea to monitor general usage patterns over time. For example, it may be the case that consumption patterns peak at certain times or it may be the case that consumption is spread over a number of timezones, creating a flatter pattern. You can perform an audit on the CDR files to obtain this information.

Index

A

Ad-hoc conferencing
- MGC systems . . . 107
- MGC-25 systems . . . 107
- RMX systems . . . 81

Avaya Communication Manager
- configure video trunks . . . 171

Avaya Meeting Exchange
- configure . . . 115

Avaya S8300 servers . . . 96, 107
Avaya S8500 servers . . . 100
Avaya S87xx servers . . . 100

H

H.320 gateway
- configure . . . 145

HDX systems
- configure . . . 62

I

IP Softphone
- configure . . . 58

M

Meeting Exchange
- configure . . . 115

MGC systems
- configure . . . 100
- configure Ad-hoc conferencing . . . 107

MGC-25 systems
- configure . . . 96, 107
- configure Ad-hoc conferencing . . . 107

P

Polycom
- HDX systems . . . 62
- MGC systems . . . 100, 107
- MGC-25 systems . . . 96, 107
- RMX systems . . . 72, 81
- V500 systems . . . 62
- VSX systems . . . 62
- VSX700 systems . . . 62

Polycom MGC
- configure as H.320 gateway . . . 145

R

RMX systems
- configure . . . 72
- configure Ad-hoc conferencing . . . 81

V

V500 systems
- configure . . . 62

video conferencing systems
- configure . . . 62, 72
- configure Ad-hoc . . . 81, 107

video trunks
- between Avaya Communication Manager systems 171

VSX systems
- configure . . . 62

VSX700 systems
- configure . . . 62