POLYCOM®

Polycom® Unified Communications Deployment Guide for the OpenScape Solution of Siemens Enterprise Communications™

| June 2011 | 3725-62124-001/A

Trademark Information

Polycom®, the Polycom "Triangles" logo, and the names and marks associated with Polycom's products are trademarks and/or service marks of Polycom, Inc., and are registered and/or common-law marks in the United States and various other countries.

All other trademarks are the property of their respective owners.

Patent Information

The accompanying product is protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

Polycom, Inc.
4750 Willow Road
Pleasanton, CA 94588-2708
USA

As between the parties, Polycom, Inc., retains title to and ownership of all proprietary rights with respect to the software contained within its products. The software is protected by United States copyright laws and international treaty provision. Therefore, you must treat the software like any other copyrighted material (e.g., a book or sound recording).

Every effort has been made to ensure that the information in this manual is accurate. Polycom, Inc., is not responsible for printing or clerical errors. Information in this document is subject to change without notice.

Contents

1 Introduction

2 Getting Started with the OpenScape Solution for Siemens Enterprise Communications

3 Use Cases from the User’s Perspective

4 Use Cases from the Network Perspective

5 Configuring Polycom HDX Systems to Interoperate with Siemens OpenScape

6 Configuring Polycom RMX Systems to Interoperate with Siemens OpenScape

1

Introduction

This document includes the requirements for the Polycom and Siemens video interoperability that Siemens refers to as Video Solution V2R2 for Siemens Enterprise Communications. The Siemens OpenScape Video V2R2 solution combines high-definition (HD) video room systems, desktop devices, and media control units with state-of-the-art unified voice and communication support by OpenScape Voice V5. OpenScape Video V2R2 also contains OpenScape Voice V4R1. This voice feature includes unified numbering plans, one directory service, support of the latest OpenScape Web Enabled (WE) or Fusion clients, and basic presence integration with OpenScape Unified Communications (UC).

OpenScape Video V2R2 offers mission-critical video. Video conferences can be provided through virtual multipoint control units (MCUs) that are highly resilient. A virtual MCU consists of multiple physical MCUs and a mechanism that controls switch-over in the event of outages and balances resource usage.

OpenScape Video combined with OpenScape Voice is a Session Initiation Protocol (SIP)-based solution. In video communications, SIP is less prevalent in voice over IP (VoIP) because most installations use H.323. The transition from H.323 to SIP is occurring as video communication progresses from standalone overlay solutions to Unified Video Conferencing (UVC) H.323 systems. Video endpoints using SIP or H.323 can be connected by IP-to-IP gateways or session border controllers (SBCs), which are also part of this solution.

Required Hardware

Siemens

- Siemens OpenScape Server that can operate in the single instance:
  - OpenScape Voice switch
  - OpenScape UC application
  - Media Server with G.711 support
- Siemens Open Stage 40 and Open Stage 60 phones

> Open Stage 20 and 40 phones have the same software. Open Stage 60 and 80 have the same software. 20/40 and 60/80 are similar but not the same.

Polycom

- Polycom® Converged Management Application™ (CMA®) 5000 Server
- Polycom® Distributed Media Application™ (DMA™) 7000 Server
- Polycom® HDX® Series Systems
- Polycom® RMX® 1500/2000/4000
- Polycom® VVX® 1500
- Polycom® Real Presence™ Experience, (RPX™), Polycom® Architected Telepresence Experience™ (ATX™), and Polycom® OTX™ or Polycom Open Telepresence Experience™ (OTX™)

Prerequisites

The following prerequisites must be met before you set up and install the Polycom and Siemens components in the Siemens OpenScape environment:

- Previous knowledge of and experience with the Siemens OpenScape components
- Access to Siemens OpenScape product documentation and relevant software
- Previous knowledge of and experience with Polycom CMA, Polycom DMA, Polycom HDX Systems, Polycom RMX systems, Polycom VVX phones, and Polycom RPX, ATX, and OTX components
- Access to the Polycom product documentation and relevant software

Supported Versions

The following tables list the supported Polycom and Siemens OpenScape versions or releases that have been tested and verified in a lab environment.

Polycom Product	Release
CMA 5000	5.5 and later
DMA 7000	2.3
Polycom HDX Series Systems	3.0.1 and later
Polycom RMX 1500/2000/4000	7.2.1
Polycom VVX 1500	3.3.1 and later
Polycom Telepresence RPX, ATX, OTX. **Note:** For this release, Polycom ITP supports H.323 only and is reachable through the Polycom RMX IP Gateway	3.0.1

Siemens Product	Release
Siemens OpenScape Desktop Client PE	V3R2
Siemens OpenScape Desktop Client WE	V3R2
Siemens OpenScape UC	V3R2
Siemens OpenScape Voice	V5

Related Documentation

For more information about installing, configuring, and administering Polycom products, refer to the Documents and Downloads link at: www.support.polycom.com.

For more information about installing, configuring, and administering Siemens OpenScape products, refer to the related documentation at: www.siemens-enterprise.com/us/support.aspx.

For more information about Acme Packet Net-Net, refer to the related documentation at: www.support.acmepacket.com/documentation.asp. You need to set up a user account to access the documentation.

Support

For Siemens Video solution issues contact your Siemens support representative.

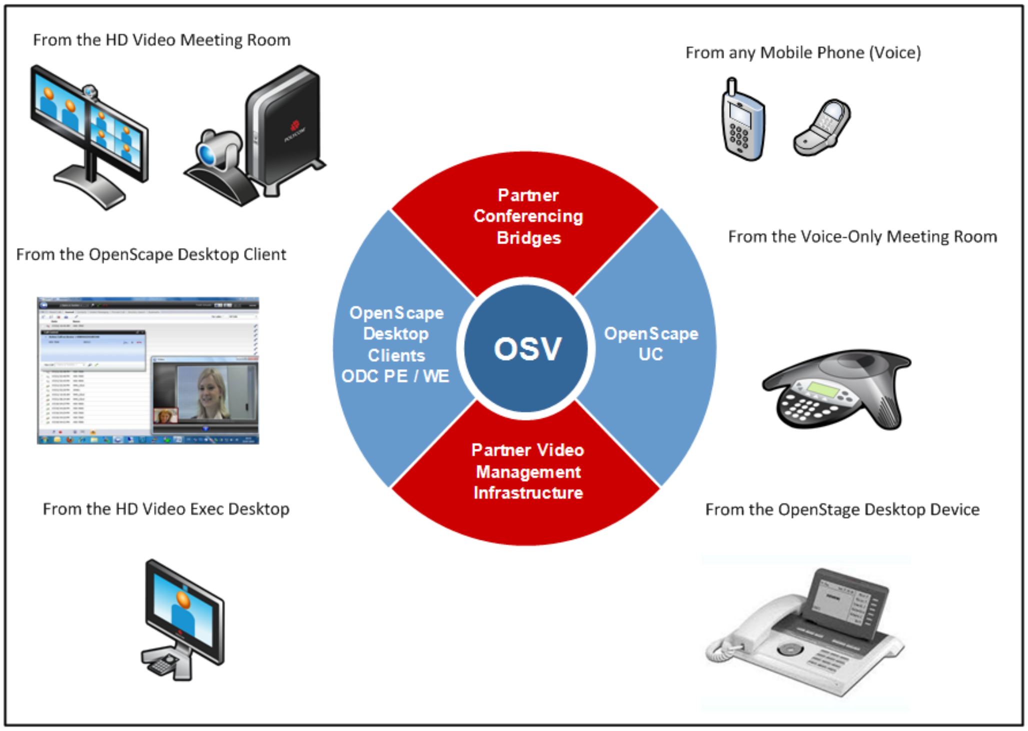
For Polycom product equipment issues, contact Polycom Global Services or www.support.polycom.com.

2

Getting Started with the OpenScape Solution for Siemens Enterprise Communications

Introduction to OpenScape Video

Video communications is a key component in unified communication and collaboration (UCC) environments. The term Unified Video Conferencing (UVC) is used to describe the integration of video into UCC. The following figure shows an overview of the OpenScape Video V2R2 deployment solution.


From the HD Video Meeting Room
From any Mobile Phone (Voice)
Partner Conferencing Bridges
From the OpenScape Desktop Client
From the Voice-Only Meeting Room
OpenScape Desktop Clients ODC PE / WE
OSV
OpenScape UC
Partner Video Management Infrastructure
From the HD Video Exec Desktop
From the OpenStage Desktop Device

OpenScape Video V2R2 Solution Features

The OpenScape Video V2R2 solution has the same look and feel for video calls and conferences as that of OpenScape UC audio solutions. Video calls are set up in the same way as voice calls — by dialing a phone number. The same clients used for audio can be used for video. The end user can start or stop showing video by pressing a button. Using video benefits from the UC functionality offered for voice, for example by using the same contact list with basic presence information.

Video endpoints can collaborate with other video or audio devices such as Open Stage desktop phones, mobile handsets, and smartphones including iPhones or Android-based phones.

OpenScape Video also offers the opportunity to add SIP-based LifeSize video endpoints to HiPath4000.

Siemens Enterprise Communications product, En*tera*sys® Secure Networks™, combined with OpenScape Video delivers location service for telepresence end systems in Polycom solutions and inventory. It also provides detection, authentication, and authorization of telepresence end systems independent from network vendor.

OpenScape Video and Open Scape Voice Integration

OpenScape Video with OpenScape Voice V4R1/V5 and OpenScape UC V3R2 support these features:

- Video calls to and from:
  - OpenScape Desktop Client PE V3.2 client
  - Polycom VVX 1500 V3.3.1 and later
  - Polycom HDX V3.0.1 series
  - Polycom RMX V7.2.1
- Video clients and endpoints can establish calls by dialing an E.164 number or 5 digits. Buddy lists and global address books are available for video calls.

OpenScape UC Integration

- Video calls to and from OpenScape Desktop Client WE V3.2 are supported.
- Video calls to and from an Open Scape Fusion client are supported.

- Video endpoints show device presence status. All allowed contacts are informed about busy or idle states.
- Video endpoints can be selected as preferred devices for incoming and outgoing calls.
- Simple presence information is supported.
- Collaboration is possible with other video devices or audio devices such as Open Stage desktop phones, any mobile handset, and any smartphone including iPhones or Android-based phones.

OpenScape Desktop Clients

OpenScape Desktop Client PE V3.2 client, OpenScape Desktop Client WE V3.2 client, and Fusion client support:

- Full HD capable desktop video solution
- Media-escalation — voice to video for OpenScape Desktop Client WE in combination with collaboration; voice first, then both sides escalate to video

Video calls use the same clients as for audio. It is not necessary for end users to learn new procedures; they can press a button to start or stop showing video.

Interdomain Video

OpenScape Video V2R2 provides interdomain video connections for video users assigned to the organization’s OpenScape Video system. Examples of users are employees working in their home offices or those traveling who want to participate remotely in video conferences from a hotel, customer premise, or a Wi-Fi hotspot, for example. Open Scape Video V2R2 provides two different methods for providing interdomain video. One is through a session border controller (SBC) or gateway mode, and the other is through a virtual private network (VPN).

SBC-Based Interdomain Video

Incoming and outgoing SIP calls between OSV SIP users in the public and in a private domain through Acme Packet Net-Net 3820. This applies to all SIP endpoints released with OpenScape Video V2R2.

VPN-Based Interdomain Video

Incoming and outgoing SIP calls between OSV SIP users in the public and in a private domain can be connected to the home private network by VPN, for example, using MobileXpress.

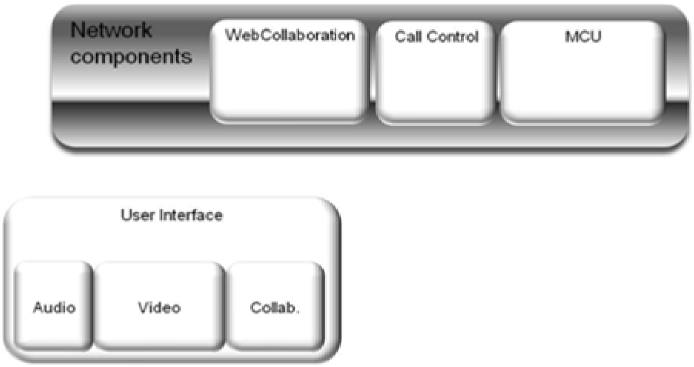
En*tera*sys in Combination with OpenScape Video

En*tera*sys allows location services for Polycom video endpoints. It streamlines inventory management and endpoint detection. Enterasys provides a way to authenticate and authorize video room and desktop systems independent from the network vendor. This feature reduces operational costs by automated asset information updates, detection of unauthorized end systems, and an automated add, move, and change process. It also allows enhanced asset management, because device types are automatically detected and tracked. This management feature improves reliability and security of video calls and conferences. QoS and security profiles can be automatically assigned.

3

Use Cases from the User’s Perspective

This chapter describes the major use cases from an end user’s perspective that are supported in OpenScape Video V2. The following figure shows the Network components and User Interface.



The Network components area includes these buttons: Web Collaboration, Call Control, and MCU. The User Interface area includes these buttons: Audio, Video, and Collab (Collaboration).

An organization’s network contains the following main areas:

- An area that users access through a user interface
- A centralized network component area (servers) that provide services and features to the end users

The centralized servers provide functionality to run specific services in the network.

Unified Video communications for enterprises usually include the following services:

- A call control system that is responsible for setting up voice or video connections based on a dialed E.164 number
- A Media Control Unit (MCU) that allows the integration of several video streams from video endpoints in a video conference

- A collaboration application server that supports users in a video or audio conference to share data or presentations or to jointly collaborate on a single document

The user interface supports equipment for the following activities:

- To listen and speak, for example, phones, mobile phones, loudspeakers, room systems
- To show videos or record videos and visuals, for example, webcams, computer-screens, mobile-cams, LCD screens, HD-room cameras
- To present or collaborate on specific data, for example, documents, spreadsheets, slides, virtual white boards

These example scenarios are shown in the following illustration:

Audio
Video
Collab.

The behavior of a group of users differs depending on the number of people and parties that are communicating. These are described as follows:

- One-to-one site — One person communicates with another person or a group in front of a single system. In this case, animated conversation and intensive interaction on varying topics and media are possible.
- Few sites — Up to eight people or groups using individual systems can watch or listen and talk to several presenters and collaborate on a project.
- Many sites — 10 to 300 persons or groups most likely watch and listen to one or a few speakers and presenters and might comment by instant messages or e-mail.

The User Interface consists of different types of desktop and room scenarios, where desktop and room systems are mainly used for one-to-one site communications. Desktop- or client-based systems at the low end often do not support high definition cameras and display controls as more high-end systems do.

Client-based systems with webcams might not be connected to high-end video room systems or to an immersive telepresence environment, although this is changing. Because of advanced technology, individual mobile and desktop interfaces can communicate with high-end room and immersive systems. Video is becoming more affordable for everyone, not only for the executive-level personnel of an organization. Requirements for video conferencing differ on the level of supported services, features, and flexibility that they require and provide for various levels of end-user interface configurations.

The user equipment usually includes microphones and speakers for audio, cameras and video display for video, and a computer for collaboration. Depending on the flexibility of specific video devices, one or more pieces of equipment are required to allow the use of all three — audio calls, video calls, and collaboration.

Video Collaboration

OpenScape Video supports two different types of collaboration — content sharing and web collaboration.

Content Sharing

Content sharing can be one conference participant presenting some type of content to the conference attendees. The participant showing content might add specific live contributions while presenting the interactions to the attendees. The content can be shared through an MCU such as the Polycom RMX platform, which mixes the presentation content received by the presenting computer to the remaining video conference callers. The participants can watch the presentation through their video displays.

Content sharing can also be used as sub-functionality of a Open Scape Web Collaboration application.

Web Collaboration

With web collaboration, a group of conference attendees jointly collaborate on the same document. The interaction can be controlled and structured by the OpenScape Web Collaboration application that connects the interacting computers through the Open Stage Web Collaboration server. One of the participant's computers can share the content to the remaining (passive) conference callers by connecting the specific computer to an MCU.

Video Room Systems

Video room systems are usually set up in conference or meeting rooms. Depending on the number of chairs, room systems offer smaller or larger video screens and sometimes even multiple screens. Room systems can also be set up and used in non-office settings such as surgical teaching rooms and small classrooms to provide video interaction with remote participants. The following figure shows an example video room system.

Room systems provide a variety of cameras from in-screen cameras to highly sophisticated camera systems. The more technically sophisticated cameras can automatically track movement to allow focusing on the current speaker. It is important that meeting planners select the right solution for the specific meeting room. Variations of possible room systems are described in the following sections.

Room Systems for 10 or More Participants

Room systems such as the Polycom HDX series system support audio, video, and content sharing in one system. Distortion-free voice and sound-and-stereo surround audio technology separate room sounds into left and right channels, giving a sense of the physical location of opposite-end participants.

For media-rich group presentations, room systems enable users to display rich-media content and data, enhancing collaboration and audience participation. Combining HDX series systems with collaboration technology allows presenters to insert their video images into projected content to more clearly explain key elements to participants.

Polycom HDX systems are typically installed in more spacious meeting rooms where a large number of people can participate. Participants can also use a computer to collaborate in parallel. Room logistics allow the connection of one of the participant's computers to the Polycom HDX system to integrate the particular content into the video streams. The following figure shows an example room system for 10 or more participants.

Room Systems for 3 to 10 Participants

This scenario applies to smaller rooms. The room system supports high-quality audio and display control, and a computer is used to support collaboration, such as sharing documents. The system typically provides only one video screen and a computer screen is used to share the content view. The computer is connected to the room system such as a Polycom HDX system to integrate the content plus video so that parties in other locations can see the content. The following figure shows an example room system for a smaller group of participants.

Desktop Video Systems

In many cases video conference participants sit at their desks in their offices and use a video desktop device such as a Polycom VVX 1500 for voice and video and a laptop to share presentations. The following figure shows an example of a participant using a VVX 1500 phone system.

The Polycom VVX 1500 can also be used at home or in a hotel. Those who have access only to a voice device can listen to the audio through the desktop audio phone or mobile phone and watch the presentation on the computer screen. Participants are visible to the rest of the participants by using an attached webcam. The caller can interact in a collaborative session at the same time or present content. Remote participants can be connected to the home network either through a VPN, such as a Mobile Express client, or through an SBC device.

A person who travels often might want to participate in a video-based web learning seminar and can listen and talk and see and be seen by using an OpenScape Desktop Client WE client and a webcam. Collaboration is possible by using the e-learning group, for example, the OpenScape Web collaboration application.

Point-to-Point Video and Small Conference Connections

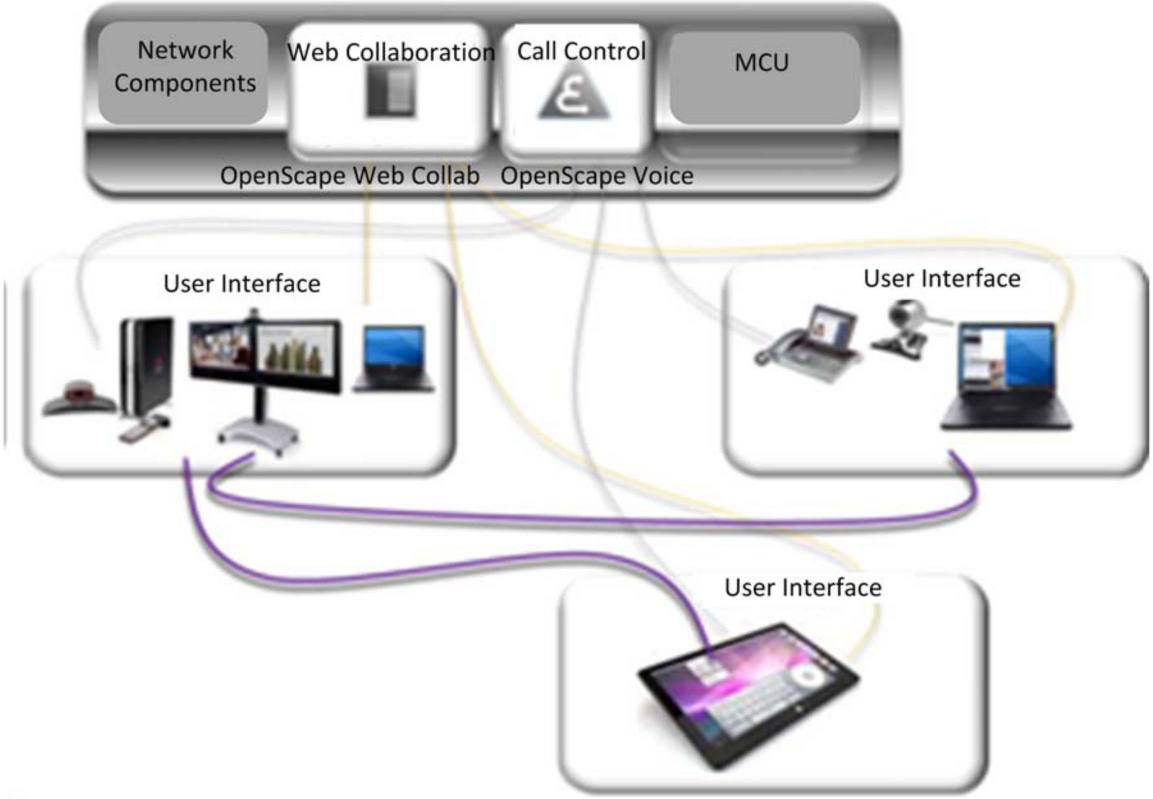
This section describes the typical use cases of end users in a Unified Video environment.

The most basic use case to is the point-to-point video call where one user connects to a second user by dialing that person’s number.

Centralized Call Control allows point-to-point voice and video calls to be established directly between involved endpoints. During the call the users can also start a collaboration controlled by a centralized server based on http/https.

Similar to point-to-point connections, small video conferences with up to eight participants can be established without the need of a centralized MCU. The video real-time transport protocol (RTP) payload can be integrated locally on a room system. Not having to have an MCU is economical. Many video conferences have fewer than eight participants and do not require the investment of a MCU for these use cases. The MCU power can be saved for large video conferences.

The following illustration shows an example of a small conference collaboration:



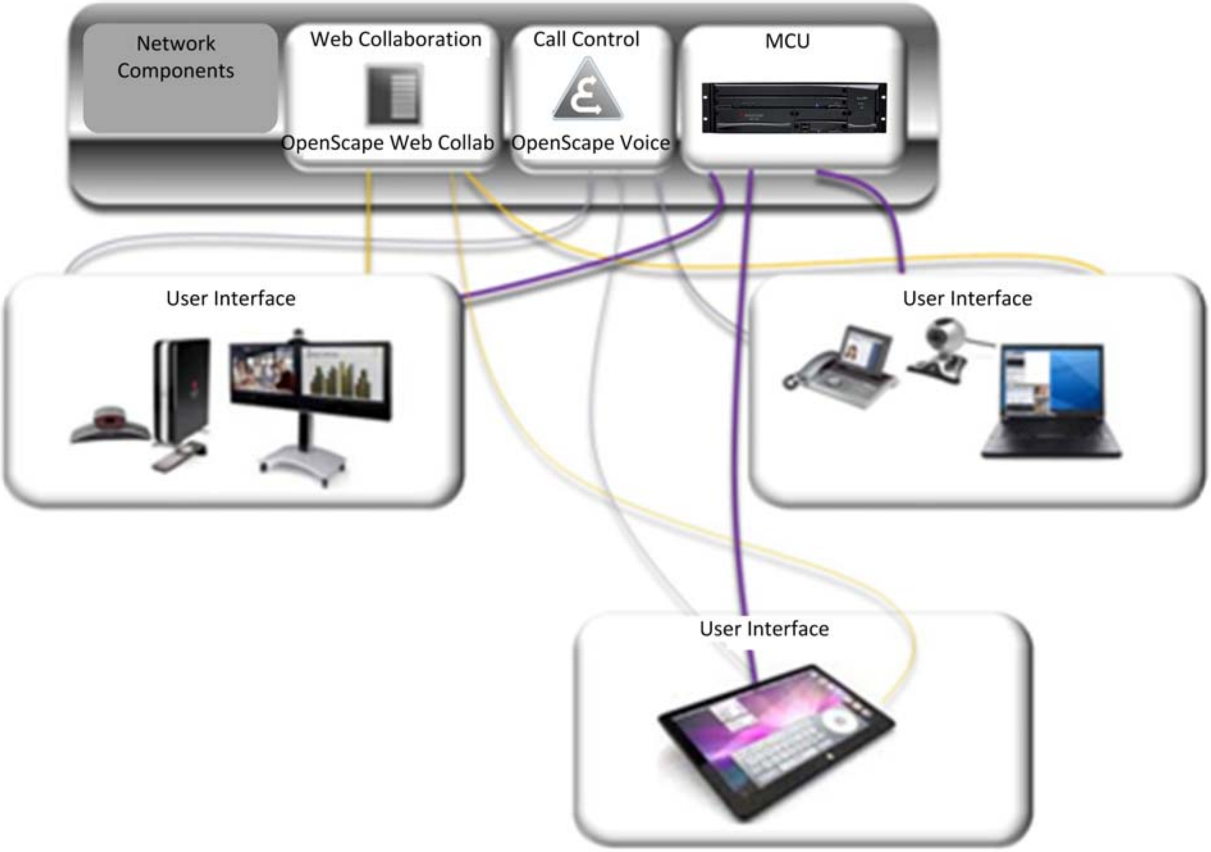
The example shows a small video conference and collaboration between the following entities where the Video streams are integrated within the Polycom HDX 8000 system:

- A Polycom HDX room system and a computer
- An OpenScape Desktop Client or Fusion client
- A tablet application

This example illustrates how different video endpoint users can jointly collaborate while having the opportunity to speak to and listen to each other, and to see each other's faces.

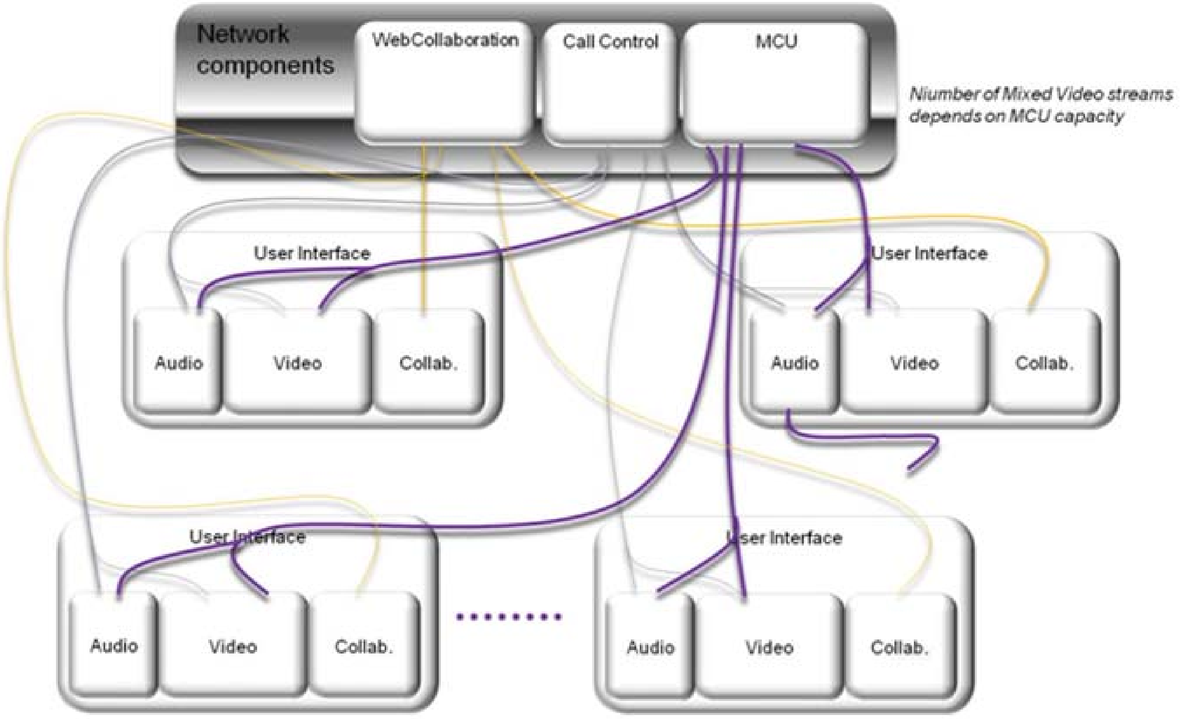
Multipoint (Three or More) Video Meetings on an MCU (Host or Participant)

Small video conferences can also be mixed with a centralized Polycom RMX, as shown in the following figure. Such a scenario has several advantages. The RMX can mix the content to the video in a way that each participant of the conference can see the presented content without using a computer. A video conference that uses only desktop video systems and no room systems can easily be established through an MCU.

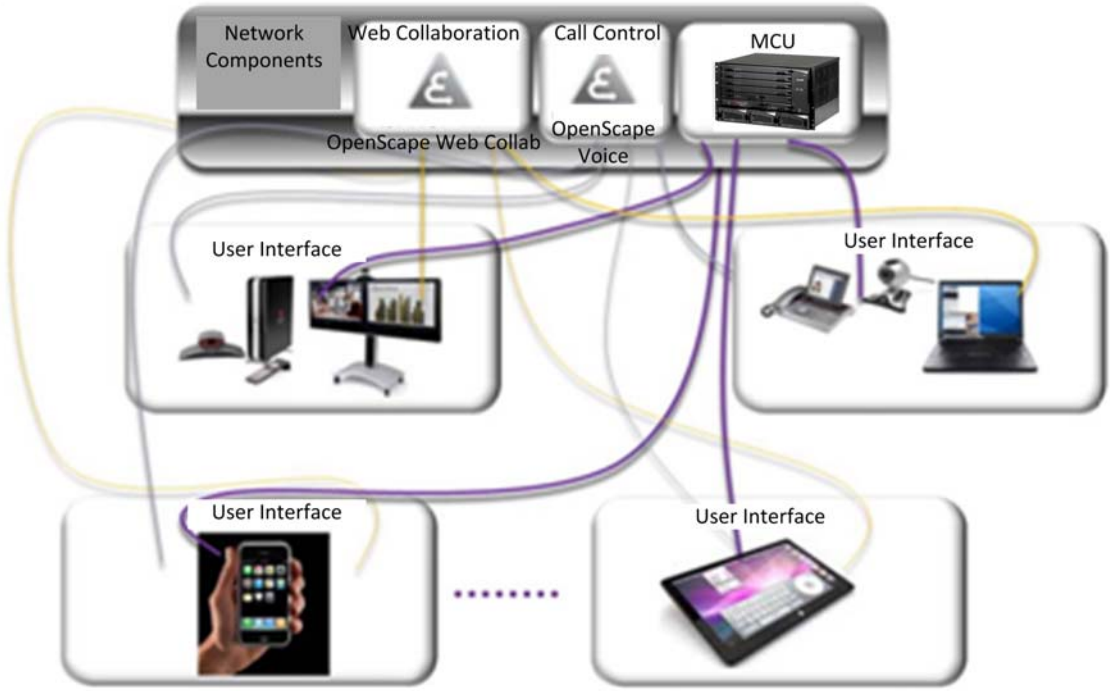


The example configuration shows a Polycom HDX room system in conference with a OpenScape Desktop or Fusion client and a digital device application user. In this case the video streams are mixed within the Polycom RMX.

The Polycom RMX can mix many more video streams and add audio-only participants, for example cell phone callers, to a large or very large conference. The next figure shows the abstract scenario of a large or very large conference. A large video conference with up to 300 members can take place for mixed environments including audio-only user interfaces, room systems, OpenScape Desktop Client or Fusion clients, digital device applications, and personal digital assistant (PDA) devices or mobile handsets.



Mixed rich-media collaboration sessions including UC clients that support audio and video, room video conferencing systems, desktop video conferencing systems, audio-only systems (telephones and soft clients) can be easily established and managed because of the powerful management systems and one-touch user interfaces. This is shown in the following figure.



The video conference with a large number of participants in this example is mixed within the Polycom RMX. Collaboration is possible using the OpenScape Web Collaboration application between the room system, OpenScape Desktop Client or Fusion client plus computer, digital device application, and PDA. Plain audio endpoints can also participate in the conference, for example through cell phones or any desk phone.

Support of Media Escalation

Media escalation is a feature of the OpenScape Desktop Client that allows users to start a video call or video conference as an audio-only connection and then manually switch to video. Participants can call in by audio and join as video participants when they are ready, which can be useful in some situations when a caller is not yet ready to be seen on video.

Mixed Rich-Media Collaboration Sessions

Mixed rich-media collaboration sessions are established between UC clients that support audio and video, room video conferencing systems, desktop video conferencing systems, and audio-only systems such as telephones and mobile phones.

In cases where web collaboration capabilities cannot be supported on the room system, a computer with collaboration capabilities can be connected to the room system such as a Polycom HDX 7000 system. The HDX 7000 system sends the video and computer information as two video streams to the MCU (RMX 1500/2000/4000) to mix the streams into one resulting video stream. The other conference partners can see both streams in one of their displays.

An example conference and collaboration might include the following:

- A Polycom HDX 7000 room system
- A Polycom RMX 2000
- An OpenScape Desktop Client or Fusion client and OpenScape Web Collaboration on a computer
- A Polycom HDX series system with a computer for OpenScape Web Collaboration

The video streams are mixed within the Polycom RMX 2000, and the video-enabled UC clients participate in telepresence meetings. The video call is established by dialing the number of the MCU using E.164 format. This is similar to dialing into a traditional audio conference. The OpenScape Voice server is in charge of the call control for the audio and video calls. The actual collaboration is controlled by a centralized application server through a web application such as OpenScape Web collaboration through http or https.

Video Systems Available in a UC Client's Address Book or Buddy List

Video endpoints, as all other audio endpoints, have been given an E.164 number and are members in the dialing plan of an enterprise. Thus, they are entries in the global directory and can be added to any personal address book or buddy lists.

Presence Information for Video Endpoints

Assuming all users have listed their video endpoints in the OpenScape WE client, they can assign their video equipment such as the Polycom HDX 7000 system to handle the presence status in current UC audio environments. The user can then adjust the presence state accordingly such as in a conference.

Connecting Non-SIP Video Systems to SIP Video

The use cases described so far are based on the assumption that all video and audio endpoints and clients support SIP signaling. However, many video solutions are based on H.323 signaling, some on proprietary signaling, and others on legacy ISDN non IP systems. Some video solutions are based on both H.323 and SIP.

OpenScape Video solutions strategically connect every video endpoint. OpenScape Video can adapt, extend, or overlay existing video deployments with its SIP-based OpenScape UC solutions.

H.323 Video Endpoints Connected to OpenScape Video V2

H.323 video endpoints are connected to the OpenScape Video V2R2 solution based on SIP signaling. A Polycom RMX can connect H.323 video to SIP-based video endpoints of OpenScape Video V2R2.

Non-IP Video Endpoints Connected to OpenScape Video V2

Legacy video endpoints (H.320) or even proprietary protocols (such as legacy telepresence) can connect to OpenScape Video V2R2 through an H.320 to a H.323 or SIP gateway. This can be based on a Polycom RMX, which also offers an H.320 to SIP or H.323 interface, but does not support a dial-through functionality.

4

Use Cases from the Network Perspective

This chapter explains specific functions that are required for end-to-end video communication solutions.

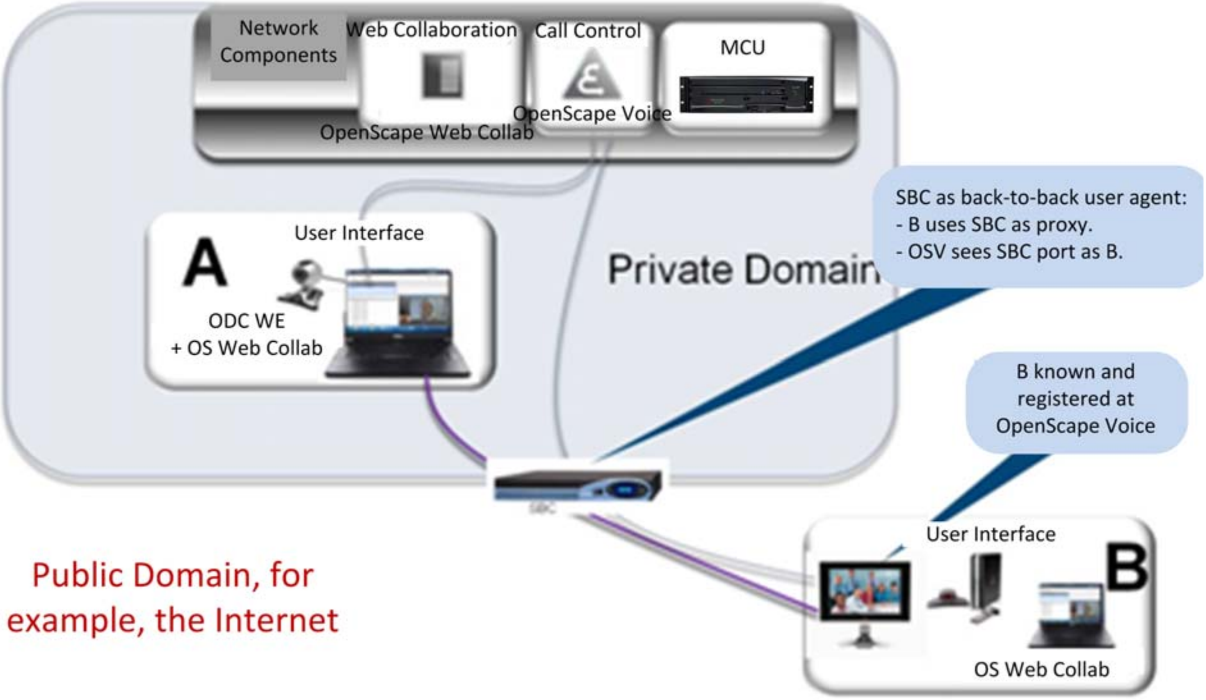
Interdomain Video Solutions

Video solutions are not always isolated domains and need to support interdomain video calls. OpenScape Video V2R2 provides SBC-based interdomain video and gateway-based interdomain video.

SBC-Based Interdomain Video

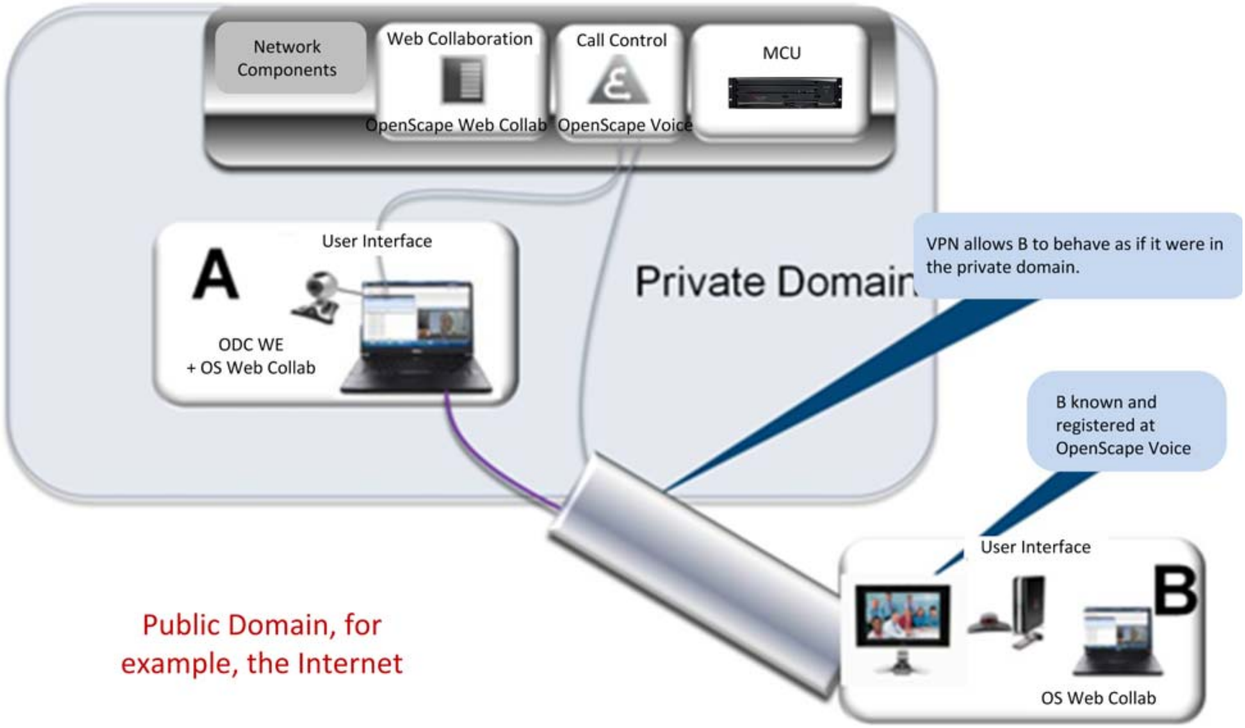
The typical use case is when one organization uses two or more video room systems to allow video conferences among their separate locations within a campus or site area. Some participants might not be available on the campus, but would be interested in joining the video call from their home, a hotel, or any off-campus location, for example by using a Polycom RMX located in the organization’s network.

Another example is a caller using a campus video system who wants to call a salesperson at a customer premise and add him or her to an established conference. Both the on-campus and off-campus parties are registered through the on-campus OpenScape Video. This scenario requires an SBC to handle the network address translation (NAT) between the two connected domains and is shown in the following figure.



VPN-Based Interdomain Video

Using a virtual private network (VPN) is another way to connect remote workers in a video conference from their home offices or those who might be traveling. The following figure shows a VPN-based interdomain video solution.



The major benefit for users in scenario B is that they can behave and use services and applications exactly the same as if they were located in the private domain.

Gateway-Based Interdomain Video

The gateway-based interdomain video includes the following major requirements:

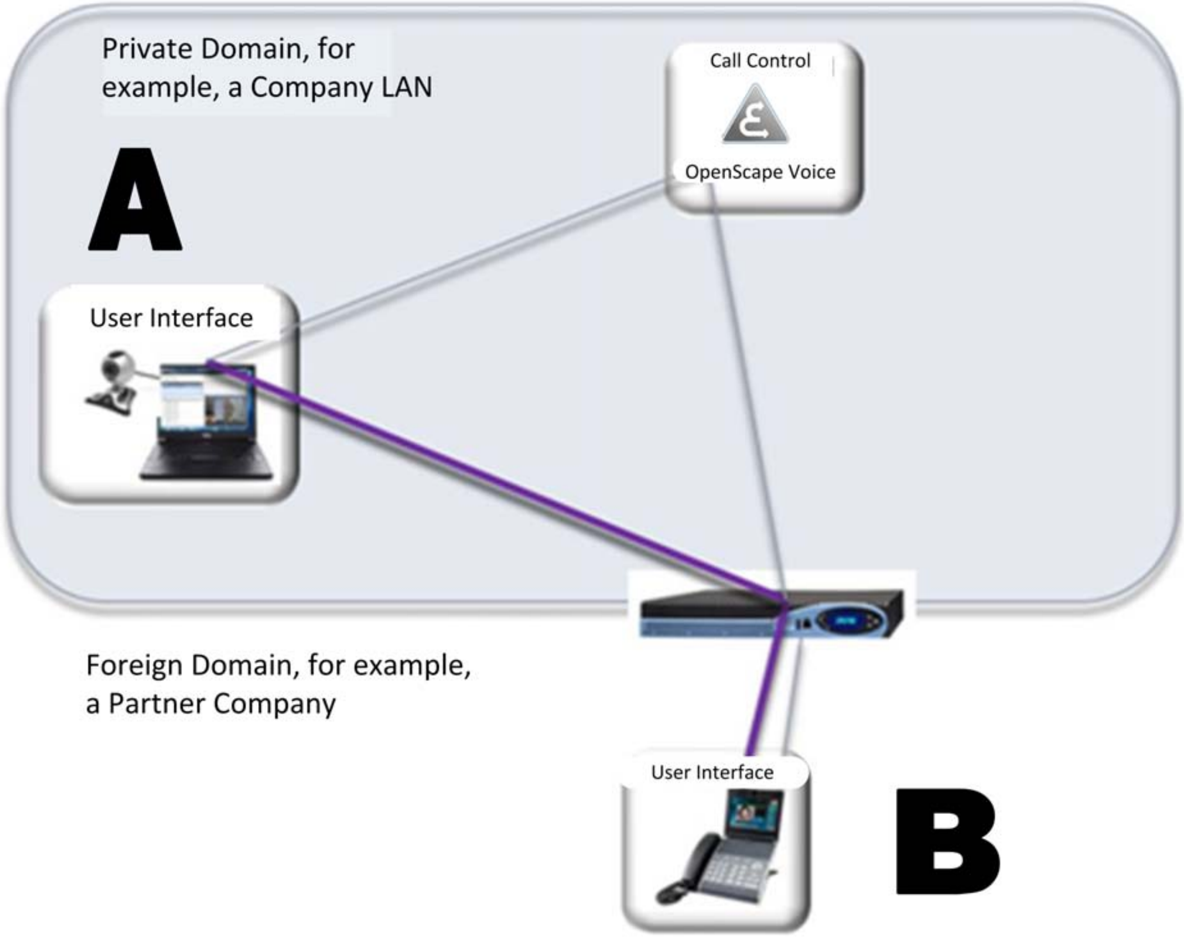
- Point-to-point video between video endpoints registered at different SIP registrars, for example, a video partner call between an OpenScape product and a Polycom employee.
- Multipoint video between video endpoints registered at different SIP registrars with an on-campus MCU, for example, a video partner conference call between an OpenScape product and Polycom on a bridge hosted by a Siemens Enterprise Communications product.

- Multipoint video between video endpoints registered at different SIP registrars with an off-campus MCU, for example, a video partner conference call between an OpenScape product and Polycom on a bridge hosted by Polycom.

In all of these use cases, the involved parties are registered at different SIP registrars, for example, the Siemens Enterprise Communications employees at an OpenScape Video within Siemens Enterprise Communications and the Polycom employees at an OpenScape Video hosted by Polycom.

Point-to-Point Video of Video Endpoints Registered at Different SIP Registrars

The following figure shows an example of point-to-point video of video endpoints registered at different SIP registrars:

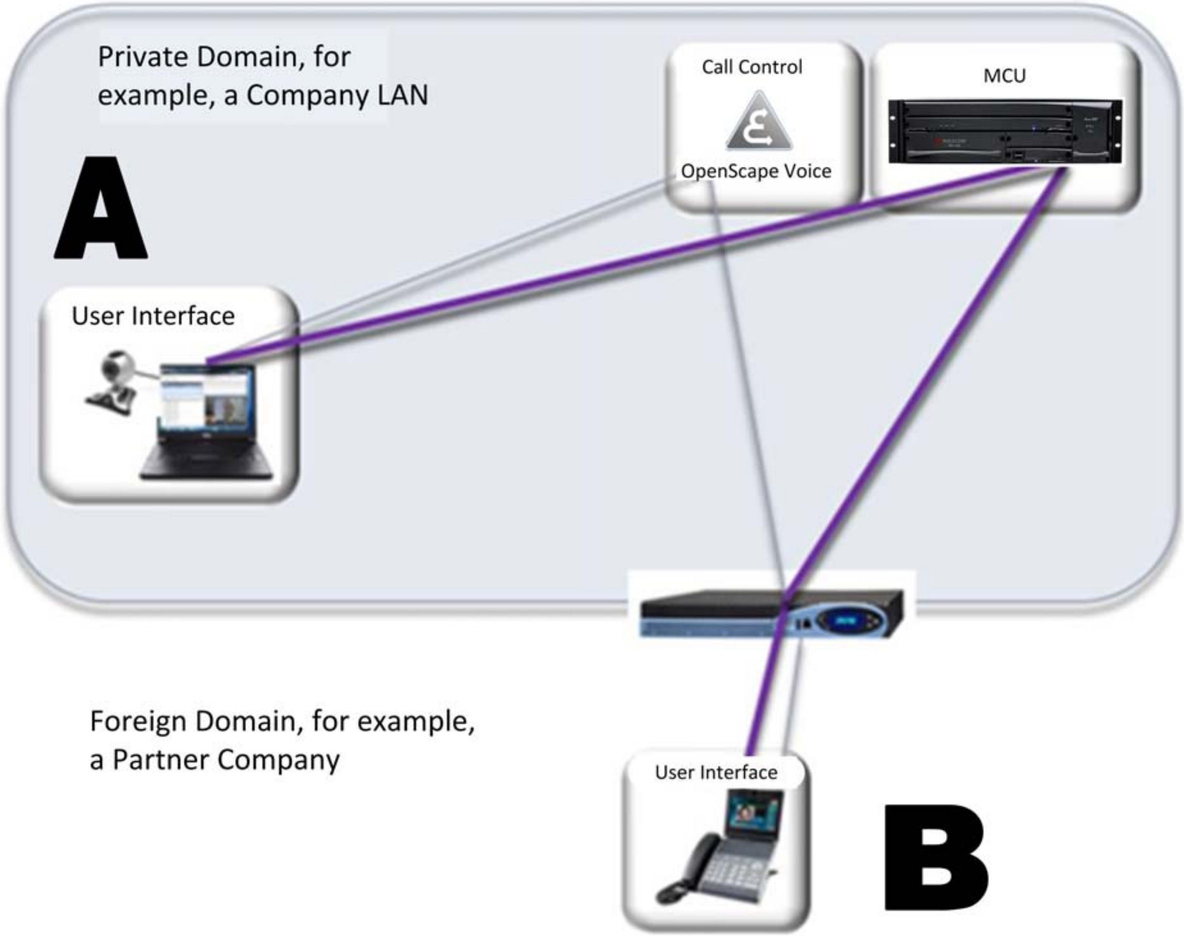

Private Domain, for example, a Company LAN
Call Control
OpenScape Voice
A
User Interface
Foreign Domain, for example, a Partner Company
User Interface
B

This figure shows a typical video point-to-point call, initiated by an end user in the private domain A, for example, siemens-enterprise.com. It can also be intimated by an endpoint B in a partner company domain, for example, polycom.com.

The incoming call, from B to A in the private domain, is established by dialing the domain_name@private domain.com, for example, 27111@siemens-enterprise.com. The outgoing call, from A to B, is established by dialing the gateway number, for example, 99 plus the domain name of the called partner, for example, 99 13131. After receiving the number, the gateway deletes 99 from the string and adds @polycom.com. The called party is addressed by 13131@polycom.com.

Multipoint Video of On-Campus Video Endpoints

The following figure shows an example of multipoint video of video endpoints that are registered at different SIP registrars with an on-campus MCU.

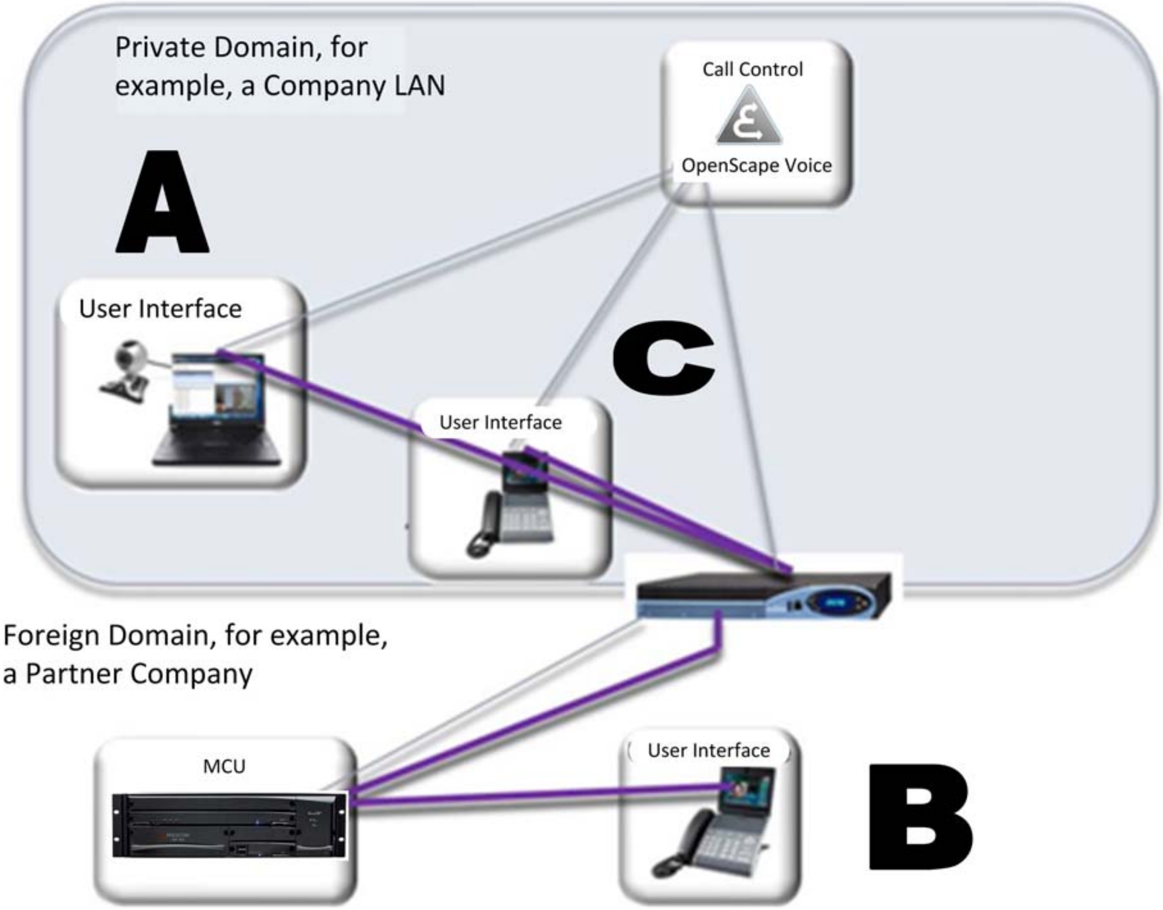

Private Domain, for example, a Company LAN
A
Call Control
OpenScape Voice
MCU
User Interface
Foreign Domain, for example, a Partner Company
User Interface
B

The figure shows an example of another typical video configuration. Two or more partners from two different companies, such as Siemens Enterprise Communications and Polycom, want to meet on an MCU in the private domain, such as siemens-enterprise.com.

User A calls into the MCU by using its domain name, for example, 88888. User B dials into the MCU by dialing domain_name@private domain.com, for example, 88888@siemens-enterprise.com.

Multipoint Video of Off-Campus Video Endpoints

The following figure shows an example of multipoint video of video endpoints that are registered at different SIP registrars with an off-campus MCU.

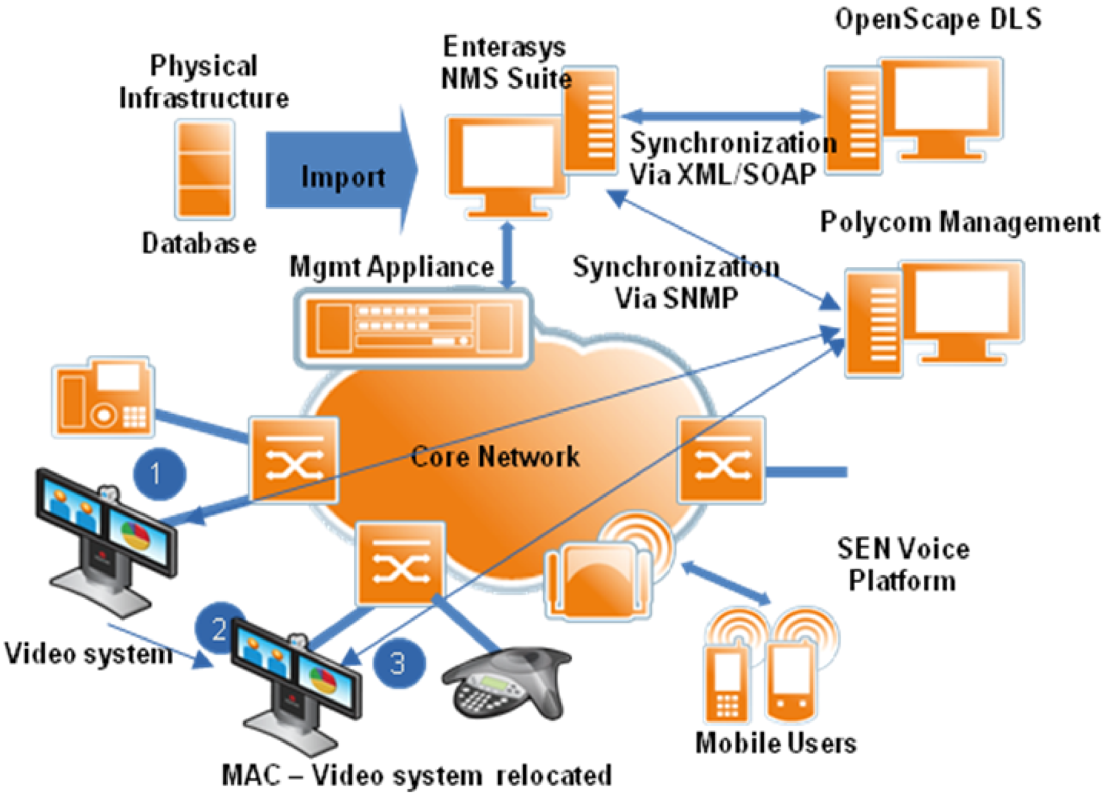

Private Domain, for example, a Company LAN
Call Control
OpenScape Voice
A
User Interface
C
User Interface
Foreign Domain, for example, a Partner Company
MCU
User Interface
B

The figure shows an example of another typical video configuration. Two or more partners from two different companies, such as SEN and Polycom, want to meet on an MCU in the private domain, such as siemens-enterprise.com.

Users A and C call into the MCU at Polycom by dialling the gateway number, for example 99 plus the DN of the called partner, that is 99 77777. After receiving the number the gateway deletes 99 from the string and adds @polycom.com. Hence the MCU is addressed with 77777@polycom.com. User B can either dial domain_name@partner domain, that is, 77777@polycom.com, or just dial 77777.

OpenScape LIA Network Automation Support for Polycom Video Endpoints

Because the number of enterprise services and applications are continually increasing, the demand for greater flexibility, mobility, and reliability has also increased. The following figure shows a location and identity assurance (LIA) network automation supported by Polycom endpoints.



The OpenScape LIA solution provides a constantly updated and automated real-time asset and location service information database for all kinds of end-user systems. This is true even in cases where the end users are new or have moved or been reconfigured.

This feature helps to reduce operational costs while increasing the productivity of administrators and users. Higher availability and reliability guarantees continuity of business processes for enterprises. OpenScape LIA improves the reliability and security of the video calls and conferences by automatically assigning QoS and security profiles (also known as Policies) using a network access control (NAC) solution.

Quality of Service

Quality of Service (QoS) is an important prerequisite for VoIP and Video over IP. The challenge is to guarantee that packet traffic and media connections are not delayed or dropped because of interferences from other lower priority traffic.

Things to consider in relation to QoS are the following:

- Latency — delay for packet delivery
- Jitter — variations in delay of packet delivery
- Packet loss — too much traffic in the network, which causes the network to drop packets

End users are affected by non-existing QoS measures such as large delays or echoes in audio connections and disturbing artifacts or even stuck video connections. In fact, the mechanisms applied to preserve QoS for VoIP and Video over IP are quite similar. Thus, OpenScape Video V2R2 relies and reuses the measures to provide QoS by OpenScape Video.

OpenScape LIA allows for automatically assigning and tracking QoS profiles for all OpenScape Video endpoints from Polycom.

Virtual MCUs in OpenScape Video V2R2

Polycom® Distributed Media Application™ (DMA™) 7000 allows configuration of virtual MCUs. These might consist of two or more physical MCUs, such as Polycom RMX or others, which can be accessed as one single MCU. One benefit of this solution is better scalability, load balance, and network simplification. The major advantage is support for mission critical video conferencing.

The DMA system identifies any failure of a physical MCU or data path and automatically switches to an alternative MCU. The end user experiences only a brief period of still video, then the conference continues.

Mission Critical Video Conferencing

Redundant MCUs through the Polycom DMA System

The Polycom DMA system, shown in the following illustration, allows control of several MCUs, such as a Polycom RMX or others, as if they were one virtual MCU. The DMA system balances the load to each connected MCU. It prevents loss of service if a bridge is down, and only the capacity of the virtual MCU is reduced.

The DMA system also supports conference call failover if a connection to bridge fails during a call. The DMA system automatically holds the call and reestablishes the connection to another bridge. Video conference participants notice little break in video and might see only a short period of still video while the system is reconnecting.

The capability of the DMA system to allow control of a Polycom RMX and another type of MCU supports migration scenarios from the Polycom RMX to another manufacturer's MCU or vice versa.

Refer to the following section for more information on the major use cases supported by the DMA system in relation to preserving mission critical video conferencing.

Use Cases Provided for Resilient Video Conferencing

Centralized Conference Resource Management

A centralized conference resource management application is needed to create a pool of conference servers that behave as one large conference server. This management application server tracks the incoming calls and routes them to the appropriate resource, for instance, based on available server resources but also based on available bandwidth to the location of this server.

If the virtual meeting room (VMR) is using a template that has cascading enabled, the application server would automatically create cascading links. The DMA system must have site topology data. For more information, refer to the Polycom DMA documentation at www.support.polycom.com.

Cascading a conference across multiple MCUs can conserve bandwidth and is especially useful when using WAN links. Participants can connect to MCUs that are geographically near them, reducing network traffic between sites to a single link to each MCU. Cascading does, however, impact the quality of the conference experience.

> Cascading is supported only for RMX MCUs and only in H.323. The Polycom DMA system must be configured to support H.323 signaling in order to enable cascading. For conferences with cascading enabled, the system selects only RMX MCUs that have H.323 signaling enabled.

The management application provides uninterrupted service by routing calls around failed or busy media servers. It also allows media servers to have a “busy – out” status during maintenance activities. From the user’s point of view, the service is always available. The system can gradually grow from small deployments of one-to-two media servers to large deployments with many geographically dispersed media servers. System administrators can monitor daily usage and plan the expansion as necessary.

This approach also provides a centralized mechanism to deploy a front-end application to control and monitor conferencing activities across all media servers. The management application acts as a load balancer in this scenario, that is, it can distribute the load over a group of conference servers. The larger the resource pool, the more efficient the load balancing function, a feature that is critical to large organizations with offices and conference servers around the world.

The same technology can be used by service providers who offer conference services globally by using the Polycom DMA 7000 solution and deploying conference servers in central points of the network. The scenario works well in architectures such as SIP, where the Registrar function is separate from the Proxy function, that is, where the endpoint is registered with a SIP Registrar in the network but sends its calls to a pool of SIP Proxies.

Automatically Route Around Outages

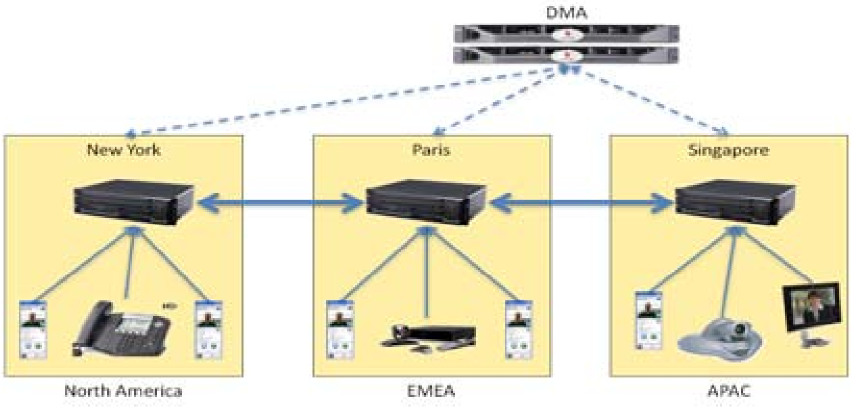
The Polycom DMA system receives notification if a bridge goes down or becomes full, and responds to prevent loss of service. Only the capacity is reduced during the outage.

In the case of a Conference Call Failover, that is, if a connection to a bridge fails during a call, the DMA system automatically holds the call and reestablishes it on another bridge. End users and administrators do not have to intervene.

Some features of the Polycom DMA system are listed in the following table.

Feature	Description
Scalability - Smart Capacity Growth	• Addition of another DMA server for redundancy • Add more MCUs • Provisioning of VMRs the same as for Medium deployment
Supported MCU Capacities	• DMA supports up to 64 bridges • Supports 1,200 concurrent calls: Video, audio, CIF, HD • Tested to 375,000 Active Directory users • Supports Polycom RMX 1500/2000/4000 bridges • Also applicable for Codian
MCU Auto Cascading	• All users dial same VMR number, regardless of location • DMA system routes calls to the closest bridge • DMA system establishes links between bridges • Users do not have to modify their dialing behaviors

An example of using DMA as a centralized conference resource management application is shown in the following figure:



5

Configuring Polycom HDX Systems to Interoperate with Siemens OpenScape

This chapter provides an overview of how to set up and configure Polycom HDX systems to interoperate with Siemens OpenScape products. For more detailed information about configuring HDX Systems, refer to the documentation on this web site: www.support.polycom.com.

Polycom HDX systems running software version 3.0.1 and later can place and receive calls with Siemens OpenScape Desktop Client PE and Desktop Client WE and with Siemens OpenScape Voice versions 3.2 and 5.

Configuring Polycom HDX Systems LAN Properties

The instructions in this section are for configuring HDX systems LAN properties when setting them up to interoperate in a Siemens OpenScape environment. Refer to the *Polycom HDX Systems Administrator's Guide* for more information on setting up Polycom HDX systems.

To configure Polycom HDX LAN properties:

1 Do one of the following:

- In the local interface, go to **System > Admin Settings > LAN Properties** (select ▶ if necessary).
- In the web interface, go to **Admin Settings > LAN Properties**.

2 Configure these settings on the LAN Properties screen:

Setting	Description
IP Address (IPv4)	Specifies how the system obtains an IP address. • **Obtain IP address automatically** — Select if the system gets an IP address from the DHCP server on the LAN. • **Enter IP address manually** — Select if the IP address will not be assigned automatically. Changing this setting causes the system to restart.
IP Address	If the system obtains its IP address automatically, this area displays the IP address currently assigned to the system. If you selected **Enter IP Address Manually**, enter the IP address here. Changing the IP address causes the system to restart.
Subnet Mask	Displays the subnet mask currently assigned to the system. If the system does not automatically obtain a subnet mask, enter one here. Changing this setting causes the system to restart.
Default Gateway (IPv4)	Displays the gateway currently assigned to the system. If the system does not automatically obtain a gateway IP address, enter one here. Changing this setting causes the system to restart.
IP Address (IPv6)	Specifies how the system obtains an IP address. • **Obtain IP address automatically** — Select if the system gets an IP address automatically. DHCP is not currently supported for IPv6. When you choose this setting, the system uses Stateless Address Autoconfiguration (SLAAC) to obtain a global address, unique local address (ULA), or site-local address using router advertisements. The network routers also must be configured appropriately to provide the advertisement packets. • **Enter IP address manually** — Select if the IP address will not be assigned automatically. • **Off** — Select to disable IPv6. Changing this setting causes the system to restart.

Setting	Description
Link-Local	Displays the IPv6 address used for local communication within a subnet.
Site-Local	Displays the IPv6 address used for communication within the site or organization.
Global Address	Displays the IPv6 internet address.
Default Gateway (IPv6)	Displays the gateway currently assigned to the system. If the system does not automatically obtain a gateway IP address, enter one here. Changing this setting causes the system to restart.
Host Name	Indicates the system's DNS name. Changing this setting causes the system to restart.
Domain Name	Displays the domain name currently assigned to the system. If the system does not automatically obtain a domain name, enter one here.
DNS Servers	Displays the DNS servers currently assigned to the system. If the system does not automatically obtain a DNS server address, enter up to four DNS servers here. • IPv6: You can specify IPv6 DNS server addresses for IP addresses entered manually or obtained automatically (in the case of a system on a hybrid network that obtains IPv4 DNS server addresses via DHCPv4). • IPv4: You can specify IPv4 DNS server addresses only when the IPv4 address is entered manually. When the IPv4 address is obtained automatically, the DNS Server addresses are also obtained automatically. Changing this setting causes the system to restart.
LAN Speed	Specify the LAN speed to use. Note that the speed you choose must be supported by the switch. Choose **Auto** to have the network switch negotiate the speed automatically. Choosing **Auto** automatically sets **Duplex Mode** to **Auto**. If you choose **10 Mbps**, **100 Mbps**, or **1000 Mbps** you must set **Duplex Mode** to **Half** or **Full**. **Note**: Polycom does not support **Auto** for the Polycom HDX system only or the switch only; the settings for both must be the same. Changing this setting causes the system to restart.

Setting	Description
Duplex Mode	Specify the duplex mode to use. Note that the Duplex mode you choose must be supported by the switch. Choose **Auto** to have the network switch negotiate the Duplex mode automatically. Choosing **Auto** automatically sets **LAN Speed** to **Auto**. The duplex settings for both the Polycom HDX system and the switch must be the same. Polycom recommends that you set both to Auto. IEEE802.3 also recommends that you use Autonegotiation to avoid network issues. Changing this setting causes the system to restart.
Enable EAP/802.1X	Specifies whether EAP/802.1X network access is enabled. Polycom HDX systems support the following authentication protocols: • EAP-MD5 • EAP-PEAPv0 (MSCHAPv2) • EAP-TTLS • EAP-TLS
Identity	Specifies the system’s identity used for 802.1X authentication. This setting is available only when EAP/802.1X is enabled.
Password	Specifies the system’s password used for 802.1X authentication. This setting is available only when EAP/802.1X is enabled.
Enable 802.1p/Q	Specifies whether VLAN and link layer priorities are enabled.
VLAN ID	Specifies the identification of the Virtual LAN.This setting is available only when 802.1p/Q is enabled. The value can be any number from 1 to 4094.
Video Priority	Sets the link layer priority of video traffic on the LAN. Video traffic is any RTP traffic consisting of video data and any associated RTCP traffic. This setting is available only when 802.1p/Q is enabled. The value can be any number from 0 to 7, although 6 and 7 are not recommended.

Setting	Description
Audio Priority	Sets the priority of audio traffic on the LAN. Audio traffic is any RTP traffic consisting of audio data and any associated RTCP traffic. This setting is available only when 802.1p/Q is enabled. The value can be any number from 0 to 7, although 6 and 7 are not recommended.
Control Priority	Sets the priority of control traffic on the LAN. Control traffic is any traffic consisting of control information associated with a call: • H.323 — H.225.0 Call Signaling, H.225.0 RAS, H.245, Far End Camera Control • SIP — SIP Signaling, Far End Camera Control, Binary Floor Control Protocol (BFCP) This setting is available only when 802.1p/Q is enabled. The value can be any number from 0 to 7, although 6 and 7 are not recommended.
Enable PC LAN Port	Specifies whether the PC LAN port is enabled on the back of a Polycom HDX 4000, Polycom HDX 7000, Polycom HDX 8000 series, or Polycom HDX 9006 system. Disable this setting for increased security.

The following IPv4 and IPv6 settings are available only on the web interface. Changing any of these settings causes the system to restart.

Setting	Description
Ignore Redirect Messages	Enables the HDX system to ignore redirect messages from network routers. A redirect message tells the endpoint to use a different router than the one it is using.
ICMP Transmission Rate Limit (millisec)	Specifies the minimum number of milliseconds between transmitted packets. Enter a number between 0 and 60000. The default value of 1000 signifies that the system sends 1 packet per second. If you enter 0, the transmission rate limit is disabled. This setting applies only to “error” ICMP packets. This setting has no effect on "informational" ICMP packets, such as echo requests and replies.
Generate Destination Unreachable Messages	Generates a `Destination Unreachable` message if a packet cannot be delivered to its destination for reasons other than network congestion.
Respond to Broadcast and Multicast Echo Requests	Sends an Echo Reply message in response to a broadcast or multicast Echo Request, which is not specifically addressed to the HDX system.

Specifying SIP Settings

If your network supports the Session Initiation Protocol (SIP), you can use SIP to connect IP calls.

To specify SIP Settings:

1 Do one of the following:

- In the local interface, go to **System > Admin Settings > Network > IP > SIP Settings** (select ▶ if necessary**.**)
- In the web interface, go to **Admin Settings > Network > IP Network > SIP Settings.**

2 Configure these settings:

Setting	Description
Transport Protocol	Indicates the protocol the system uses for SIP signaling. The SIP network infrastructure in which your Polycom HDX system is operating determines which protocol is required. **Auto** enables an automatic negotiation of protocols in the following order: TLS, TCP, UDP. This is the recommended setting for most environments. **TCP** provides reliable transport via TCP for SIP signaling. **UDP** provides best-effort transport via UDP for SIP signaling. **TLS** provides secure communication of the SIP signaling. TLS is available only when the system is registered with a SIP server that supports TLS. When you choose this setting, the system ignores TCP/UDP port 5060.
User Name	Specifies the SIP address or SIP name of the system — for example, mary.smith@department.company.com. If you leave this field blank, the system's IP address is used for authentication. In a Siemens environment, this setting is the Subscriber number provided by the OpenScape Voice administrator.
Domain User Name	Specifies the name to use for authentication when registering with a SIP Registrar Server — for example, msmith@company.com. If the SIP proxy requires authentication, this field and the password cannot be blank.

Setting	Description
Password	Specifies the password that authenticates the system to the Registrar Server.
SIP Registrar Server	Specifies the IP address or DNS name of the SIP Registrar Server. By default for TCP, the SIP signaling is sent to port 5060 on the registrar server. By default for TLS, the SIP signaling is sent to port 5061 on the registrar server. Enter the IP address and port using the following format: <IP_Address>:<Port> *<IP_Address>* can be an IPv4 address or a DNS hostname such as `servername.company.com:6050`. Hostnames can resolve to IPv4 or IPv6 addresses. Syntax Examples: • To use the default port for the protocol you have selected: 10.11.12.13 • To specify a different TCP or UDP port: 10.11.12.13:5071 Enter an IPv6 address using the following format: [*<IPv6_Address>*]:*<Port>* An example of an IPv6 address is: [2001:db8:85a3::8a2e:370:7334]:8032:8033
Proxy Server	Specify the DNS name or IP address of the SIP Proxy Server. If you leave this field blank, the Registrar Server is used. If you leave both the SIP Registrar Server and Proxy Server fields blank, no Proxy Server is used. By default for TCP, the SIP signaling is sent to port 5060 on the proxy server. By default for TLS, the SIP signaling is sent to port 5061 on the proxy server. The syntax used for this field is the same as for the SIP Registrar Server field.

Points to note about SIP:

The SIP protocol has been widely adapted for voice over IP communications and basic video conferencing; however, many of the advanced video conferencing capabilities are not yet standardized. Many capabilities also depend on the SIP server.

Examples of features that are not supported using SIP are:

- Cascaded multipoint is not supported in SIP calls.
- For more information about SIP compatibility issues, refer to the *Release Notes for Polycom HDX Systems*.

Specifying H.323 Settings

If your network uses a gatekeeper, the system can automatically register its H.323 name and extension. This allows others to call the system by entering the H.323 name or extension instead of the IP address.

To specify H.323 settings:

1 Do one of the following

- In the local interface, go to **System > Admin Settings > Network > IP > H.323 Settings**.
- In the web interface, go to **Admin Settings > Network > IP Network > H.323 Settings.**

2 Configure these settings on the H.323 Settings screen:

Setting	Description
Display H.323 Extension	Allows users to enter H.323 extensions separately from the gateway ID on the Place a Call screen. If your system is registered with a gatekeeper, this setting also displays your H.323 extension on the home screen. If you do not select this setting, users make gateway calls by entering the call information in this format: gateway ID + ## + extension
H.323 Name	Specifies the name that gatekeepers and gateways use to identify this system. You can make point-to-point calls using H.323 names if both systems are registered to a gatekeeper. The H.323 Name is the same as the System Name, unless you change it. Your organization’s dial plan may define the names you can use.
H.323 Extension (E.164)	Lets users place point-to-point calls using the extension if both systems are registered with a gatekeeper, and specifies the extension that gatekeepers and gateways use to identify this system. Your organization’s dial plan may define the extensions you can use.

Configuring the System to Use a Gatekeeper

A gatekeeper manages functions such as bandwidth control and admission control. The gatekeeper also handles address translation, which allows users to make calls using static aliases instead of IP addresses that may change each day.

To configure the system to use a gatekeeper:

1 Do one of the following:

- In the local interface, go to **System > Admin Settings > Network > IP > H.323 Settings** (select ▶ if necessary).
- In the web interface, go to **Admin Settings > Network > IP Network > H.323 Settings**.

2 Configure these settings:

Setting	Description
Use Gatekeeper	Select this setting to use a gatekeeper. Gateways and gatekeepers are required for calls between IP and ISDN. • **Off** — Calls do not use a gatekeeper. • **Auto** — System attempts to automatically find an available gatekeeper. • **Specify** — Calls use the specified gatekeeper. This option must be selected to enable H.235 Annex D Authentication. • **Specify with PIN** — Calls use the specified E.164 address and require an **Authentication PIN**.
H.323 Name	Specifies the name that gatekeepers use to identify this system. You can make point-to-point calls using H.323 names if both systems are registered to a gatekeeper. The H.323 Name is the same as the System Name, unless you change it. Your organization's dial plan may define the names you can use.
H.323 Extension (E.164)	Specifies the extension that gatekeepers and gateways use to identify this system. Your organization's dial plan may define the extensions you can use.

Setting	Description
Primary Gatekeeper IP Address	• If you chose **No** for the **Use Gatekeeper** field, the **Primary Gatekeeper IP Address** field is not displayed. • If you chose to use an automatically selected gatekeeper, this area displays the gatekeeper’s IP address. • If you chose to specify a gatekeeper, enter the gatekeeper’s IP address or name (for example, `gatekeeper.companyname.usa.com`, or `10.11.12.13`). The primary gatekeeper IP address contains the address with which the system registers. As part of the gatekeeper registration process, the gatekeeper might return alternate gatekeepers. If communication with the primary gatekeeper is lost, the HDX system registers with the alternate gatekeeper but continues to poll the primary gatekeeper. If the system reestablishes communications with the primary gatekeeper, the HDX system unregisters from the alternate gatekeeper and reregisters with the primary gatekeeper.
Authentication	Enables support for H.235 Annex D Authentication. When H.235 Annex D Authentication is enabled, the H.323 gatekeeper ensures that only trusted H.323 endpoints are allowed to access the gatekeeper.
User Name	Specifies the user name for authentication with H.235 Annex D.
Password	Specifies the password for authentication with H.235 Annex D.
Use PathNavigator for Multipoint Calls	Lets you specify whether multipoint calls use the system’s internal multipoint capability or the Conference on Demand feature available with Polycom PathNavigator™, Readi*Manager* SE200, or Polycom CMA system. This feature is available only if the system is registered with one of these gatekeepers.

Some gatekeeper settings are read only. In the local interface go to **System > Admin Settings > Network > IP > H.323 Settings** (select ▶ if necessary) or **Admin Settings > Network > IP Network > H.323 Settings** in the web interface to view the following settings:

— **Current Gatekeeper IP Address**

— **Primary Gatekeeper IP Address**

— **Alternate Gatekeepers**
These are gatekeepers that the system can use if the primary gatekeeper is not available. Supported gatekeepers include the Polycom PathNavigator™ gatekeeper.

Points to note about Polycom's Conference on Demand feature:

In order to place calls using Conference on Demand, you need to:

- Register your Polycom HDX system with a Polycom gatekeeper. A Polycom RMX® system must be configured with the gatekeeper to provide the Conference on Demand feature.
- Enable Use PathNavigator for Multipoint Calls.
- Create a group in the directory (recommended).

When using Conference on Demand:

- Once the call begins, you cannot add another site to the call — even if the site was in the call originally.
- The Polycom RMX system must have enough ports available to complete the call.

Configuring the System to Use a Gateway

A gateway performs code and protocol conversion between H.323 (IP), SIP, and H.320 (ISDN), so that users on different networks can call one another. If the system is configured to use a gateway, you must also configure it to use a gatekeeper. For more information, refer to Configuring the System to Use a Gatekeeper on page 5-9.

To configure the system to use a gateway:

1 Do one of the following:

   – In the local interface, go to **System > Admin Settings > Network > IP > H.323 Settings** (select ▶ if necessary)**.**

   – In the web interface, go to **Admin Settings > Network > IP Network > H.323 Settings.**

2 Configure these settings:

Setting	Description
Country Code	Specifies the country code for the system's location.
Area Code	Specifies the area or city code for the system's location.
Number	Specifies the gateway's number.
H.323 Extension (E.164)	Specifies the extension that identifies this system for incoming gateway calls. The default H.323 Extension can be changed.

Setting	Description
Gateway Number Type	Specifies the number type users enter to call this system: • **Direct Inward Dial** — Users enter an internal extension to call this system directly. **Note**: If you choose this setting, you must also register the number with the gatekeeper as an E.164 alias. • **Number + Extension** — Users enter the gateway number and the system's extension to call this system.
Number of Digits in DID Number	Specifies the number of digits in the DID number. The national or regional dialing plan for your location determines the standard number of digits. For instance, the US standard is 7 digits.
Number of Digits in Extension	Specifies the number of digits in the extension used when **Direct Inward Dial** is selected. Your organization's dial plan determines this number.

3 Enter a prefix or suffix for each bandwidth you want to allow for gateway calls.

The use of suffixes and prefixes is dependent on the gatekeeper, gateway capability, and gateway configuration. Associating prefixes and suffixes with particular bandwidths on your gateway can optimize the use of bandwidth by your organization. Be sure the gateway is configured to use the same prefixes and suffixes you define for the system.

6

Configuring Polycom RMX Systems to Interoperate with Siemens OpenScape

This chapter provides an overview of how to set up and configure Polycom RMX 1500/2000/4000 systems to interoperate with Siemens OpenScape products. For more detailed information about configuring Polycom RMX, refer to the Polycom RMX documentation on this web site: www.support.polycom.com.

IP Network Services

To enable the Polycom RMX system to function within the IP network environment, you need to define the network parameters for the IP Network Services. You can access the configuration dialog boxes for the network services through the RMX Management pane of the RMX Web Client.

Two IP network services are defined for the Polycom RMX:

- Management Network
- Default IP Service (Conferencing Service)

When using the RMX system with multiple services, five IP networks are required for the RMX 4000 and three IP networks are required for the RMX2000 and RMX 1500.

Dial in, dial out connections and RMX management are supported within the following IP addressing environments:

- IPv6
- IPv4
- IPv6 & IPv4

When IPv4 is selected, IPv6 fields are not displayed and conversely when IPv6 is selected, IPv4 fields are not displayed. When IPv6 & IPv4 is selected both IPv6 and IPv4 fields are displayed.

Mandatory System Flags

The following mandatory System Flags must be set:

- SIP_FREE_VIDEO_RESOURCES NO

  This setting is required because the OpenScape Desktop Client escalates from Audio to Video.

- ENABLE_SIP_PPC_FOR_ALL_USER_AGENT YES

  This setting is required to enable Binary Floor Control Protocol (BFCP), which enables content over SIP, between the RMX and the HDX system.

- ENABLE_FLOW_CONTROL_REINVITE NO

  This flag is related to enable BFCP.

Management Network (Primary)

The Management Network is used to control the Polycom RMX, mainly through the RMX Web Client application. The Management Network contains the network parameters, such as the IP address of the Control Unit, that are needed to connect the RMX and the RMX Web Client. This IP address can be used by the administrator or service personnel to connect to the Control Unit if the RMX becomes corrupted or inaccessible.

You can create a private network during First Time Power-up by using either a USB key or a cable to set the Management Network parameters.

For more information, refer to the P*olycom RMX 1500/2000/4000 Administrator's Guide* and the *RMX 1500/2000/4000 Getting Started Guide*.

Default IP Service (Conferencing Service)

The Default IP Service (Conferencing Service) is used to configure and manage communications between the Polycom RMX and conferencing devices such as endpoints, gatekeepers, SIP servers, and so forth.

The Default IP Service contains parameters for the following:

- Signaling Host IP Address
- MPM+ and MPMx boards (media processors)
- External conferencing devices

Calls from all external IP entities are made to the Signaling Host, which initiates call set-up and assigns the call to the appropriate MPM+ or MPMx board.

Conferencing related definitions such as environment (H.323 or SIP) are also defined in this service.

Most of the Default IP Service is configured by the Fast Configuration Wizard, which runs automatically if the following occurs:

- First time power-up
- Deletion of the Default IP Service, followed by a system reset

> Changes made to any of these parameters only take effect when the Polycom RMX unit is reset. An Active Alarm is created when changes made to the system have not yet been implemented, which indicates that the MCU must be reset.

Modifying the Management Network

The Management Network parameters need to be modified if you want to do any of the following tasks:

- Connect directly to the RMX from a workstation
- Modify routes
- Modify DNS information

To view or modify the Management Network Service:

1 In the RMX Management pane, click **IP Network Services**.

2 In the IP Network Services list pane, double-click **Management Network**.

The Management Network Properties - IP dialog box opens.

3 Modify the following fields:

Field	Description	
Network Service Name	Displays the name of the Management Network. This name cannot be modified. **Note:** This field is displayed in all Management Network Properties tabs.	
IP Version	IPv4	Select this option for IPv4 addressing only.
	IPv6	Select this option for IPv6 addressing only.
	IPv4 & IPv6	Select this option for both IPv4 and IPv6 addressing.

Field	Description		
IPv6 Configuration Method	Auto (Stateless)	Select this option to allow automatic generation of the following addresses: • Link-Local (For internal use only) • Site-Local • Global	
	Manual	Select this option to enable manual entry of the following addresses: • Site-Local • Global Manual configuration of the following address types is not permitted: • Link-Local • Multicast • Anycast	
Control Unit IP Address	IPv4	The IPv4 address of the RMX Control Unit. This IP address is used by the RMX Web Client to connect to the RMX.	
	IPv6	The IPv6 address of the RMX Control Unit. This IP address is used by the RMX Web Client to connect to the RMX. **Note:** Internet Explorer 7™ is required for the RMX Web Client to connect to the RMX using IPv6.	
		All	Click the **All** button to display the IPv6 addresses as follows: Auto — If selected, Site-Local and Global site addresses are displayed. Manual — if selected, only the Manual site address is displayed.

Field	Description		
Shelf Management IP Address	IPv4	The IPv4 address of the RMX Shelf Management Server. This IP address is used by the RMX Web Client to monitor hardware.	
	IPv6	The IPv6 address of the RMX Shelf Management Server. This IP address is used by the RMX Web Client to monitor hardware. **Note:** Internet Explorer 7™ is required for the RMX Web Client to connect to the RMX using IPv6.	
		All	Click the **All** button to display the IPv6 addresses as follows: Auto — If selected, Site-Local and Global site addresses are displayed. Manual — If selected, only the Manual site address is displayed.
Subnet Mask	Enter the subnet mask of the Control Unit. **Note:** This field is specific to *IPv4* and is not displayed in IPv6 only mode.		
Secured Communication	Select to enable Secured Communication. The RMX supports TLS 1.0 and Secure Socket Layer (SSL) 3.0. An SSL/TLS Certificate must installed on the RMX for you to enable this feature.		

4 Click the Routers tab and modify the following fields:

Field	Description	
Default Router IP Address	IPv4	Enter the IP address of the default router. The default router is used whenever the defined static routers are unable to route packets to their destination. The default router is also used when host access is restricted to one default router.
	IPv6	

Field	Description	
Static Routes IPv4 Only Table		The system uses Static Routes to search other networks for endpoint addresses that are not found on the local LAN. Up to five routers can be defined in addition to the Default Router. The order in which the routers appear in the list determines the order in which the system looks for the endpoints on the various networks. If the address is in the local subnet, no router is used. To define a static route (starting with the first one), click the appropriate column and enter the required value.
	Router IP Address	Enter the IP address of the router.
	Remote IP Address	Enter the IP address of the entity to be reached outside the local network. The Remote Type determines whether this entity is a specific component (Host) or a network. • If Host is selected in the Remote Type field, enter the IP address of the endpoint. • If Network is selected in the Remote Type field, enter of the segment of the other network.
	Remote Subnet Mask	Enter the subnet mask of the remote network.
Static Routes IPv4 Only Table	Remote Type	Select the type of router connection: • **Network** — defines a connection to a router segment in another network. • **Host** — defines a direct connection to an endpoint found on another network.

5 Click the DNS tab and modify the following fields:

Field	Description
MCU Host Name	Enter the name of the MCU on the network. The default name is RMX.
DNS	Select: **Off** — if DNS servers are not used in the network. **Specify** — to enter the IP addresses of the DNS servers. **Note**: The IP address fields are enabled only if Specify is selected.
Register Host Names Automatically to DNS Servers	Select this option to automatically register the MCU Signaling Host and Shelf Management with the DNS server.
Local Domain Name	Enter the name of the domain where the MCU is installed.
DNS Servers Addresses:	
Primary Server	The static IP addresses of the DNS servers. A maximum of three servers can be defined.
Secondary Server	
Tertiary Server	

6 **RMX 2000 only**: Click the **LAN Ports** tab and modify the following fields:

> For the RMX 1500/4000 platforms, you can manually modify automatically identified speed and transmit/receive mode for each LAN port that the system uses if required by the specific switch in the Ethernet Settings dialog box. These settings are not part of the Management Network dialog box as for the RMX 2000.

Field	Description	
Port Speed	The RMX has 3 LAN ports. The administrator can set the speed and transmit/receive mode manually for LAN 2 Port only.	
	Port	The LAN port number: 1, 2, or 3. **Note:** Do not change the automatic setting of Port 1 and Port 3. Any change to the Port 1 speed will not be applied.
	Speed	Select the speed and transmit/receive mode for each port. Default: Auto – Negotiation of speed and transmit/receive mode starts at 1000 Mbps Full Duplex, proceeding downward to 10 Mbps Half Duplex. **Note:** To maximize conferencing performance, especially in high bit rate call environments, a 1Gb connection is recommended.

7 Click **OK**. If you have modified the Management Network Properties, reset the MCU.

Modifying the Default IP Network Service

The Default IP Service parameters need to be modified if you want to change any of the following:

- Network type that the RMX connects to
- IP address of the RMX Signaling Host
- IP addresses of the RMX Media boards
- Subnet mask of the RMX's IP cards
- Gatekeeper parameters or add gatekeepers to the Alternate Gatekeepers list
- SIP server parameters

Fast Configuration Wizard

You can use the Fast Configuration Wizard to configure the Default IP Service. The wizard starts automatically if no Default IP Network Service is defined. This happens during First Time Power-up before the service has been defined or if the Default IP Service has been deleted, followed by an RMX restart.

The IP Management Service tab in the Fast Configuration Wizard is enabled only if the factory default Management IP addresses were not modified.

If the Fast Configuration Wizard does not start automatically, the Default IP Service must be modified through the IP Network Properties dialog boxes.

To view or modify the Default IP Service:

1. Click **IP Network Services** in the RMX Management pane.
2. Double-click **Default IP Service** in the Network list pane.

   The Default IP Service - Networking IP dialog box opens.
3. Modify the following fields:

Field	Description
Network Service Name	The name Default IP Service is assigned to the IP Network Service by the Fast Configuration Wizard. This name can be changed. **Note:** This field is displayed in all IP Signaling dialog boxes and can contain character sets that use Unicode encoding.
IP Network Type	Displays the network type selected during the First Entry configuration. The Default IP Network icon indicates the selected environment. You can select: • **H.323** — For an H.323-only Network Service. • **SIP** — For a SIP-only Network Service. • **H.323 & SIP** — for an integrated IP Service. Both H.323 and SIP participants can connect to the MCU using this service. **Note:** This field is displayed in all Default IP Service tabs.
Signaling Host IP Address	Enter the address to be used by IP endpoints when dialing in to the MCU. Dial out calls from the RMX are initiated from this address. This address is used to register the RMX with a Gatekeeper or a SIP Proxy server.

Field	Description
Media Card 1 **IP Address**	Enter the IP address(es) of the media card (s) as provided by the network administrator: RMX1500: MPMx 1 RMX 2000: MPM+/MPMx 1 and MPM+/MPMx 2 (if installed) RMX 4000: MPM+/MPMx 1, MPM+/MPMx 2 (if installed), MPM+/MPMx 32 (if installed) and MPM+/MPMx 4 (if installed) Endpoints connect to conferences and transmit call media (video, voice and content) through these addresses.
Media Card 2 **IP Address** **(RMX 2000/4000)**	
Media Card 3 **IP Address** **(RMX 4000)**	
Media Card 4 **IP Address** **(RMX 4000)**	
Subnet Mask	Enter the subnet mask of the MCU. The default value is 255.255.255.0.

4 Click the Routers tab.

With the exception of IP Network Type, the field definitions of the Routers tab are the same as for the Default Management Network.

5 Click the Gatekeeper tab.

6 Modify the following fields:

Field	Description	
Gatekeeper	Select **Specify** to enable configuration of the gatekeeper IP address. When **Off** is selected, all gatekeeper options are disabled.	
Primary Gatekeeper IP Address or Name	Enter either the gatekeeper's host name as registered in the DNS or IP address.	**Note:** When in IPv4 & IPv6 or in IPv6 mode, it is easier to use Names instead of IP addresses.
Alternate Gatekeeper IP Address or Name	Enter the DNS host name or IP address of the gatekeeper used as a fallback gatekeeper used when the primary gatekeeper is not functioning properly.	
MCU Prefix in Gatekeeper	Enter the number with which this Network Service registers in the gatekeeper. This number is used by H.323 endpoints as the first part of their dial-in string when dialing the MCU. When PathNavigator or SE200 is used, this prefix automatically registers with the gatekeeper. When another gatekeeper is used, this prefix must also be defined in the gatekeeper.	

Field	Description
Register as Gateway	Select this check box if the RMX unit is to be seen as a gateway, for example, when using an alternate gatekeeper. **Note:** Do not select this check box when using the Polycom ReadiManager/CMA 5000 gatekeeper.
Refresh Registration every __ seconds	The frequency with which the system informs the gatekeeper that it is active by re-sending the IP address and aliases of the IP cards to the gatekeeper. If the IP card does not register within the defined time interval, the gatekeeper will not refer calls to this IP card until it re-registers. If set to 0, re-registration is disabled. **Note:** It is recommended to use default settings. This is a re-registration and not a ‘keep alive’ operation – an alternate gatekeeper address may be returned.
Aliases:	
Alias	The alias that identifies the RMX’s Signaling Host within the network. Up to five aliases can be defined for each RMX. **Note:** When a gatekeeper is specified, at least one prefix or alias must be entered in the table.
Type	The type defines the format in which the card’s alias is sent to the gatekeeper. Each alias can be of a different type: • H.323 ID (alphanumeric ID) • E.164 (digits 0-9, * and #) • Email ID (email address format, for example, abc@example.com) • Participant Number (digits 0 to 9, *, and #) **Note:** Although all types are supported, the type of alias to be used depends on the gatekeeper’s capabilities.

7 Click the Ports tab.

Settings in the Ports tab allow specific ports in the firewall to be allocated to multimedia conference calls. The port range recommended by the Internet Assigned Numbers Authority (IANA) is 49152 to 65535. The MCU uses this recommendation along with the number of licensed ports to calculate the port range.

8 Modify the following fields:

Field	Description
Fixed Ports	Leave this check box cleared if you are defining a Network Service for local calls that do not require configuring the firewall to accept calls from external entities. When cleared, the system uses the default port range and allocates 4 RTP and 4 RTCP ports for media channels (Audio, Video, Content and FECC). **Note:** When ICE Environment is enabled, 8 additional ports are allocated to each call. Click this check box to manually define the port ranges or to limit the number of ports to be left open.
TCP Port from - to	Displays the default settings for port numbers used for signaling and control. To modify the number of TCP ports, enter the first and last port numbers in the range. The number of ports is calculated as follows: Number of simultaneous calls x 2 ports (1 signaling + 1 control).
UDP Port from - to	Displays the default settings for port numbers used for audio and video. To modify the number of UDP ports, in *Card Configuration Mode*: Enter the first and last port numbers in the range. The number of ports is calculated as follows: **Number of simultaneous calls x 8 ports** (2 audio, 2 video, 2 Content, and 2 FECC). In MPM+/MPMx Card Configuration Mode: Enter the first and last port numbers in the range, and the range must be **1024** ports. When ICE environment is enabled, the range must be **2048** ports.

If the network administrator does not specify an adequate port range, the system accepts the settings and issues a warning. Calls are rejected when the MCU's ports are exceeded.

9 If required, click the QoS tab.

Quality of Service (QoS) is important when transmitting high bandwidth audio and video information. QoS can be measured and guaranteed in terms of:

- Average delay between packets
- Variation in delay (jitter)

– Transmission error rate

DiffServ and Precedence are the two QoS methods that the RMX supports. These methods differ in the way the packet's priority is encoded in the packet header. The way RMX implements QoS is defined per Network Service, not per endpoint.

Note: The routers must support QoS in order for IP packets to get higher priority.

10 View or modify the following fields:

Field	Description
Enable	Select to enable the configuration and use of the QoS settings. When un-checked, the values of the Differentiated Services Code Point (DSCP) bits in the IP packet headers are zero.
Type	DiffServ and Precedence are two methods for encoding packet priority. The priority set here for audio and video packets must match the priority set in the router. **DiffServ** — Select when the network router uses DiffServ for priority encoding. The default priorities for both audio and video packets is 0x88. These values are determined by the QOS_IP_VIDEO and QOS_IP_AUDIO flags in the *system.cfg* file. **Precedence** — Select when the network router uses Precedence for priority encoding, or when you are not sure which method is used by the router. Precedence needs to be combined with None in the TOS field. The default priority is 5 for audio and 4 for video packets. **Note:** Precedence is the default mode as it is capable of providing priority services to all types of routers, as well as being currently the most common mechanism.
Audio / Video	You can prioritize audio and video IP packets to ensure that all participants in the conference hear and see each other clearly. Select the desired priority. The scale is from 0 to 5, where 0 is the lowest priority and 5 is the highest. The recommended priority is 4 for audio and 4 for video to ensure that the delay for both packet types is the same and that audio and video packets are synchronized and to ensure lip sync.

Field	Description
TOS	Select the type of service (TOS) that defines optimization tagging for routing the conferences' audio and video packets. **Delay** — The recommended default for video conferencing. Prioritized audio and video packets tagged with this definition are delivered with minimal delay because the throughput of IP packets minimizes the queue sequence and the delay between packets. **None** — No optimization definition is applied. This is a compatibility mode in which routing is based on Precedence priority settings only. Select **None** if you do not know which standard your router supports.

11 Click the SIP Servers tab and modify the following fields.

Field	Description
SIP Server	Select: • **Specify** — to manually configure SIP servers. • **Off** — if SIP servers are not present in the network.
SIP Server Type	Select: **Other** — for the OpenScape environment.
Transport Type	Select the protocol that is used for signaling between the MCU and the SIP Server or the endpoints according to the protocol supported by the SIP Server: • **UDP** — Select this option to use UDP for signaling. • **TCP** — Select this option to use TCP for signaling. • **TLS** — The Signaling Host listens on secured only on port 5061, and all outgoing connections are established on secured connections. Calls from SIP clients or servers to non-secured ports are rejected. The supported protocols are TLS 1.0, SSL 2.0, and SSL 3.0.
Create Certificate	Creates a Certificate Request to be sent to a Certification Authority.
Certificate Method	Select the method for sending the Certificate to the RMX: • **CSR** • **PEM/PFX**
SIP Servers: Primary / Alternate Server Parameter	
Server IP Address	Enter the IP address of the preferred SIP server. **Note:** When in IPv4 & IPv6 or in IPv6 mode, it is easier to use Names instead of IP Addresses.

Field	Description
Server Domain Name	Enter the name of the domain that you are using for conferences, for example: `user_name@domain name` The domain name is used for identifying the SIP server in the appropriate domain according to the host part in the dialed string. For example, when a call to `EQ1@polycom.com` reaches its outbound proxy, this proxy looks for the SIP server in the `polycom.com` domain, to which it will forward the call. When this call arrives at the SIP server in `polycom.com`, the server looks for the registered user (EQ1) and forwards the call to this Entry Queue or conference.
Port	Enter the number of the TCP or UDP port used for listening. The port number must match the port number configured in the SIP server. The default port is 5060.
Outbound Proxy Servers: Primary / Alternate Server Parameter	
Server IP Address	By default, the Outbound Proxy Server is the same as the SIP Server. If they differ, modify the IP address of the Outbound Proxy and the listening port number (if required). **Note:** When in IPv4 & IPv6 or in IPv6 mode, it is easier to use Names instead of IP Addresses.
Port	Enter the port number that the outbound proxy is listening to. The default port is 5060.

12 Click the Security tab and modify the following fields:

Field	Description
Authentication User Name	Enter the conference, Entry Queue, or Meeting Room name as registered with the proxy. This field can contain up to 20 ASCII characters.
Authentication Password	Enter the conference, Entry Queue, or Meeting Room password as defined in the proxy. This field can contain up to 20 ASCII characters.

If the Authentication User Name and Authentication Password fields are left empty, the SIP Digest authentication request is rejected. For registration without authentication, the RMX must be registered as a trusted entity on the SIP server.

Ethernet Settings

For the RMX 1500/4000 platforms, you can manually modify the automatically identified speed and transmit/receive mode of each LAN port that the system uses if the specific switch requires it in the Ethernet Settings dialog box. These settings are not part of the Management Network dialog box as for RMX 2000.

RMX 1500: The Port numbers displayed in the dialog box do not reflect the physical Port numbers as labeled on the RMX 1500 MCU.

Note: On the RMX 1500, the Port numbers displayed in the dialog box do not reflect the physical Port numbers as labeled on the RMX 1500 MCU.

The physical mapping of Port Type to the physical label on the back panel of the RMX 1500 is shown in the following table.

Port Type	Label on MCU		
	1500	**4000**	
Media	LAN 2	LAN 2	RTM LAN Card
Modem	Modem	LAN 1	RTM-IP 4000 Card
Management 1	MNG B	LAN 2	
Signaling 1	MNG	LAN 3	
ShM	Shelf	LAN 6	

To modify the automatic LAN port configuration:

1 On the RMX menu, click **Setup > Ethernet Settings**.

The Ethernet dialog box opens.

Note: On the RMX 1500/4000, although the RTM LAN (media card) port is shown as Port 1 in the Ethernet Settings and Hardware Monitor fields, the physical LAN connection is Port 2.

2 Modify the following field:

Field	Description	
Speed	The RMX has 3 LAN ports on the RTM-IP (Management, Signaling, and Shelf Management), and additional LAN ports on each media card (RTM LAN) and RTM ISDN cards. The administrator can manually set the speed and transmit/receive mode for these ports.	
	Port	The LAN port number. **Note:** Do not change the automatic setting of Port 1,4 and Port 5 of the Management 2 and Signaling 2 Networks. Any change to the speed of these ports will not be applied.
	Speed	Select the speed and transmit/receive mode for each port. Default: Auto — Negotiation of speed and transmit/receive mode starts at 1000 Mbps Full Duplex, proceeding downward to 10 Mbps Half Duplex. **Note:** To maximize conferencing performance, especially in high bit rate call environments, a 1 Gb connection is recommended.

IP Network Monitoring

The Signaling Monitor is the RMX entity used for monitoring the status of external network entities such as the gatekeeper, DNS, SIP proxy, and Outbound proxy and their interaction with the MCU.

To monitor signaling status:

1 In the RMX Management pane, click **Signaling Monitor**.

2 In the Signaling Monitor pane, double-click **Default IP Service**.

The RMX CS IP tab displays the following fields:

Field	Description
Service Name	The name assigned to the IP Network Service by the Fast Configuration Wizard.

<table>
<tr><th>Field</th><th colspan="3">Description</th></tr>
<tr><td rowspan="3"><b>IPv4</b></td><td colspan="3">IP Address</td></tr>
<tr><td>Default Router IP Address</td><td colspan="2">The IP address of the default router. The default router is used whenever the defined static routers are unable to route packets to their destination. The default router is also used when host access is restricted to one default router.</td></tr>
<tr><td>Subnet Mask</td><td colspan="2">The subnet mask of the MCU.
Default value: 255.255.255.0.</td></tr>
<tr><td rowspan="4"><b>IPv6</b></td><td rowspan="3">Scope</td><td colspan="2">IP Address</td></tr>
<tr><td>Global</td><td>The Global Unicast IP address of the RMX.</td></tr>
<tr><td>Site-Local</td><td>The IP address of the RMX within the local site or organization.</td></tr>
<tr><td>Default Router IP Address</td><td colspan="2">The IP address of the default router. The default router is used whenever the defined static routers are unable to route packets to their destination. The default router is also used when host access is restricted to one default router.</td></tr>
</table>

3 Click the **H.323** tab.

The H.323 tab displays the following fields:

Field	Description
Connection State	The state of the connection between the Signaling Host and the gatekeeper: **Discovery** — The Signaling Host is attempting to locate the gatekeeper. **Registration** — The Signaling Host is in the process of registering with the gatekeeper. **Registered** — The Signaling Host is registered with the gatekeeper. **Not Registered** — The registration of the Signaling Host with the gatekeeper failed.

Field	Description	
Registration Interval	The interval in seconds between the Signaling Host's registration messages to the gatekeeper. This value is taken from either the IP Network Service or from the gatekeeper during registration. The lesser value of the two is chosen.	
	Role	Active — The active gatekeeper. Backup — The backup gatekeeper that can be used if the connection to the preferred gatekeeper fails.
	ID	The gatekeeper ID retrieved from the gatekeeper during the registration process.
	Name	The gatekeeper's host's name.
	IP Address	The gatekeeper's IP address.

4 Click the **SIP Servers** tab.

The SIP Servers tab displays the following fields:

Field	Description
Role	**Active** — The default SIP Server is used for SIP traffic. **Backup** — The SIP Server is used for SIP traffic if the preferred proxy fails.
Name	The name of the SIP server.
IP	The SIP server's IP address.
Status	The connection state between the SIP Server and the Signaling Host. **Not Available** — No SIP server is available. **Auto** — Gets information from DHCP, if used.

Using IPv6 Networking Addresses for RMX Internal and External Entities

IPv6 addresses can be assigned to both RMX (Internal) and External Entity addresses.

RMX Internal Addresses

Default Management Network Service

- Control Unit
- Signaling Host
- Shelf Management

- MPM1 (Media Card)
- MPM2 (Media Card)

External Entities

- Gatekeepers (Primary & Secondary)
- SIP Proxies
- DNS Servers
- Default Router
- Defined participants

IPv6 Guidelines

- Internet Explorer 7™ is required for the RMX Web Client and RMX Manager to connect to the RMX using IPv6.
- IPv6 is supported with MPM+ and MPMx media cards only.
- The default IP address version is IPv4.
- Internet Explorer 7 is required for the RMX Web Client use an IPv6 connection to the RMX.
- The IP address field in the Address Book entry for a defined participant can be either IPv4 or IPv6. A participant with an IPv4 address cannot be added to an ongoing conference while the RMX is in IPv6 mode nor can a participant with an IPv6 address be added while the RMX is in IPv4 mode. An error message, Bad IP address version, is displayed and the New Participant dialog box remains open so that the participant's address can be entered in the correct format.
- Participants that do not use the same IP address version as the RMX in ongoing conferences launched from Meeting Rooms, Reservations and Conference Templates, and are disconnected. An error message, Bad IP address version, is displayed.
- IP Security (IPSec) Protocols are not supported.

Licensing and System Information

System Information includes License Information, and general system information, such as system memory size and Media Card Configuration Mode.

To view the System Information properties box:

>> On the RMX menu, click Administration > System Information.

The System Information properties box is displayed.

The System Information properties box displays the following information:

Information	Description
Total Number of Video (CIF) Participants	Displays the number of CIF video participants licensed for the system.
RMX Version	Displays the System Software Version of the RMX.
ISDN/PSTN	The field value indicates whether RTM ISDN/ PSTN hardware has been detected in the system. Range: True / False
Encryption	The field value indicates whether Encryption is included in the MCU license. Encryption is not available in all countries. Range: True / False
Telepresence Mode	The field value indicates whether the system is licensed to work with RPX and TPX Telepresence room systems. Range: True / False
Serial Number	Displays the Serial Number of the RMX.
Multiple Services	A *Multiple Services* license is installed.
HD	On the RMX1500 with a MPMx-Q media card, the use of HD with Continuous Presence requires an additional license.
Polycom Partners	The field value indicates that the System Software contains features for the support of specific Polycom Partner environments.
Memory Size [MB]	This field indicates the RMX system memory size in MBytes. Possible values include the following: • **1024 MB** — Version 7.1 requires 1024 Mbytes of memory. • **500 MB** — If Memory size is 512MB, Version 7.1 is not supported. • **2048 MB** — Specify this memory size when using the RMX 4000. DO NOT upgrade the system to Version 7.1.

Information	Description
Card Configuration Mode	Indicates the MCU configuration as derived from the installed media cards: • **MPM+** — Only MPM+ cards are supported. MPMx cards in the system are disabled. • **MPMx** — Only MPMx cards are supported. MPM+ cards in the system are disabled.

When started with Version 7.0 installed, the RMX enters MPM+ mode by default, even if no media cards are installed:

- The RMX only switches between MPM+ and MPMx Card Configuration Modes if MPM+ or MPMx cards are removed or swapped while it is powered on.
- The Card Configuration Mode switch occurs during the next restart.
- Installing or swapping MPM+ or MPMx cards while the system is off will not cause a mode switch when the system is restarted - it will restart in the Card Configuration Mode that was active previous to powering down.

7

Feature Limitations

The following table lists the known feature limitations for this release. If a workaround is available, it is noted in the table.

Issue ID	Found in Release	Description	Workaround
VIDEO-89476	HDX software 3.0.1	When an HDX system that is TCP-registered to OpenScape Voice is restarted, it might not delete its registration to OpenScape Voice as it is supposed to.	None
VIDEO-88989	HDX software 3.0.1 OpenScape Video V3 R2	When an HDX system and a TANDBERG C60 are both TCP-registered to OpenScape Video, and the C60 calls the HDX system, dual video might not display.	None
VIDEO-88824	HDX software 3.0.1 OpenScape Desktop client V3R2	The HDX system might use the incorrect ports when receiving a call from the OpenScape Desktop client over the transport layer security (TLS) protocol using Multimedia Internet KEYing (MIKEY).	None
VIDEO-87603	HDX software 3.0.1	A problem monitoring SNMP might occur in the HDX system when operating in a Siemens OpenScape UC environment.	None
VNGR-21180	RMX 7.2.1	In some situations, calls to the RMX cannot be completed and the TCP connection cannot be established.	None
VNGR-20918	RMX 7.2	If an RMX separates from the network, you cannot configure the network service for the recording link.	Configure the default H.323 IP network service to the same settings as the RSS network.
VNGR-20855	RMX 7.2	Sometimes during a conference, active SIP participants are not released if the RMX is reset.	None

Issue ID	Found in Release	Description	Workaround
VNGR-20815	RMX 7.2.2	When in a call managed by the RMX 2000 with multiple networks and with HDX systems registered to the Siemens server, the interactive voice response (IVR) feature might not work correctly and content might not be viewable.	None.
VNGR-20098	RMX 7.1	When a SIP device uses RMX to dial external participants using the network separation feature, the DTMF suffix dialing over the gateway profile might not work correctly on both H.323 and SIP.	None
VNGR-19150	RMX 7.0	When OpenScape calls an RMX 2000 and sends a SIP invitation, the RMX rings but might not answer the call.	None
VNGR-19149	RMX 7.0	When OpenScape calls an RMX 2000 and successfully connects, the OpenScape desktop client might not show the RMX auto attendant or hear the announcement.	None