Design Guide for the Cisco Unified Videoconferencing Solution Using Desktop Component Release 7.1

May 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-22089-01

Design Guide for the Cisco Unified Videoconferencing Solution Using Desktop Component Release 7.1

CONTENTS

CHAPTER 1 **Selecting a Deployment Topology** 1-1

About Cisco Unified Videoconferencing Solution Deployments 1-1
- Selecting a Deployment 1-2
- Selecting a Deployment Topology 1-2
- Selecting Components 1-3

About a Basic Deployment of the Cisco Unified Videoconferencing Solution 1-4
- Basic Deployment Functionality 1-5
- Basic Deployment Limitations 1-6

About a Small Centralized Topology of the Cisco Unified Videoconferencing Solution 1-6
- Small Centralized Deployment Functionality 1-8
- Small Centralized Deployment Limitations 1-9

About a Large Centralized Topology of the Cisco Unified Videoconferencing Solution 1-10
- Large Centralized Deployment Functionality 1-11
- Large Centralized Deployment Limitations 1-12

About Large Distributed Single-zone Deployment of the Cisco Unified Videoconferencing Solution 1-12
- Large Distributed Single-zone Deployment Functionality 1-14
- Large Distributed Single-zone Deployment Limitations 1-15

CHAPTER 2 **Installing and Upgrading Components of the Cisco Unified Videoconferencing Solution** 2-1

Prerequisites for Installing the Cisco Unified Videoconferencing Solution Components 2-2
- Cisco Unified Videoconferencing Solution Installation 2-2

About Installing Cisco Unified Videoconferencing Solution Hardware Components 2-5

How to Install Cisco Unified Videoconferencing Solution Software Components 2-5
- Installing the Resource Manager Component of the Cisco Unified Videoconferencing Manager 2-6
- Installing Cisco Unified Videoconferencing Desktop Server 2-6

About Upgrades 2-6

CHAPTER 3 **Configuring Cisco Unified Videoconferencing Solution Components** 3-1

How to Configure a Cisco Unified Videoconferencing Desktop Server 3-1
- Cisco Unified Videoconferencing Desktop Server 3-2
- Cisco Unified Videoconferencing Desktop Recording Server 3-2
- Cisco Unified Videoconferencing Desktop Streaming Server 3-2
- Configuring Basic Cisco Unified Videoconferencing Desktop Server Settings 3-3
- Configuring Meeting Access Instructions 3-5

Restricting H.323 Ports between Cisco Unified Videoconferencing Desktop Server and MCU 3-5
How to Configure an MCU 3-6
Performing Basic Configuration of Cisco Unified Videoconferencing 3500 MCU 3-6
Performing Basic Configuration of the Cisco Unified Videoconferencing 5000 Series MCU 3-7
Configuring Auto-Attendant Feature in Multiple-MCU Deployments 3-8
Configuring Cisco Unified Videoconferencing 3500 Series Gateway 3-9
How to Configure Cisco Unified Videoconferencing Manager 3-11
Performing Basic Cisco Unified Videoconferencing Manager Configuration 3-11
Configuring an Auto-Attendant Session 3-15
How to Configure Solution Components for Recording 3-15
Configuring Cisco Unified Videoconferencing Desktop Server for Recording 3-16
Configuring Cisco Unified Videoconferencing Manager for Recording 3-19
Configuring a Gatekeeper 3-21
How to Configure Cisco Unified Videoconferencing Desktop Server to Allow Streaming 3-21
Desktop Server Limitations 3-22
Guidelines for Configuring Streaming in Load Balancing Deployments 3-22
Configuring This Desktop Streaming Server to Manage Streaming 3-22
Configuring an Alternate Desktop Server for Watching Webcasts 3-23
Configuring Streaming for Playback Using the UDP Connection 3-24
How to Enable Streaming Over Port 80 3-24
How to Configure Third-Party Equipment 3-26
Configuring a Firewall 3-27

CHAPTER 4

Configuring Cisco Unified Videoconferencing Desktop Servers for Scalability and High Availability 4-1

Scalability with Round Robin DNS 4-1
Round Robin DNS Functionality 4-1
Round Robin DNS Limitations 4-2
Scalability with Generic Load Balancer 4-2
Generic Load Balancer Functionality 4-2
How to Configure Round Robin DNS and Generic Load Balancers 4-2
Generic Load Balancer Limitations 4-7
Scalability with Radware WSD 4-7
Radware WSD Functionality 4-7
How to Configure Radware WSD 4-7
Radware WSD Limitations 4-11

CHAPTER 5 **Testing your Cisco Unified Videoconferencing Solution Deployment** 5-1

Testing Desktop Connectivity 5-1

Testing Room System Connectivity and Moderation 5-2

Testing Webcast Access 5-2

Testing gateway Functionality 5-3

Testing Load Balancing 5-3

Finding Further Information 5-4

APPENDIX A **Configuring Secure Connection Between Cisco Unified Videoconferencing Solution Components** A-1

About Server Certificates A-1

Configuring Secure Access to the Cisco Unified Videoconferencing Manager A-2

Configuring Secure Access to Cisco Unified Videoconferencing Desktop Server A-4

Configuring Cisco Unified Videoconferencing Desktop Server to Use HTTPS A-4

Configuring Conference Server with a Certificate A-5

Configuring Desktop Clients to Accept Generated Certificate Located on the Conference Server A-6

Configuring Secure Communication Between Cisco Unified Videoconferencing Desktop Server and Cisco Unified Videoconferencing Manager A-7

Configuring Cisco Unified Videoconferencing Desktop Server and Cisco Unified Videoconferencing Manager to Use Encryption A-7

Enabling Mutual Authentication A-8

Configuring Windows Firewall A-12

Example of Using the Microsoft Certificate Service A-13

Configure Desktop When Using Microsoft CA A-13

Generating a PKCS12 Certificate Using Microsoft Certificate Service A-14

Export the Certificate A-15

Importing the Server Certificate into the Personal Certificate Store on the Local Computer A-16

APPENDIX B **Configuring Dual-NIC Cisco Unified Videoconferencing Solution Deployments** B-1

About the Functionality of Dual-NIC Deployments B-1

Using Cisco Unified Videoconferencing Desktop Server in Dual-NIC Deployments B-2

Installing Cisco Unified Videoconferencing Desktop Server with Dual-NIC B-2

Limiting Available IP Addresses in a Dual-NIC Deployment B-3

Configuring Settings for Dual/Single-NIC Deployments B-3

Deployment Examples B-4

Configuring Cisco Unified Videoconferencing Desktop Server Network Interface B-5

Modifying Static Routing Configuration B-6

APPENDIX C **Configuring the Cisco Unified Videoconferencing Manager Prefix** C-1

APPENDIX D **Configuring a Firewall** D-1

Firewall Rules D-1

NAT Rules D-5

CHAPTER 1

Selecting a Deployment Topology

- About Cisco Unified Videoconferencing Solution Deployments, page 1-1
- About a Basic Deployment of the Cisco Unified Videoconferencing Solution, page 1-4
- About a Small Centralized Topology of the Cisco Unified Videoconferencing Solution, page 1-6
- About a Large Centralized Topology of the Cisco Unified Videoconferencing Solution, page 1-10
- About Large Distributed Single-zone Deployment of the Cisco Unified Videoconferencing Solution, page 1-12

About Cisco Unified Videoconferencing Solution Deployments

Deployments described in this chapter suit a Cisco Unified Videoconferencing Desktop Server with a single NIC. However, Cisco Unified Videoconferencing Desktop Server is designed to handle advanced topologies involving dual-NIC deployments. For information about dual-NIC deployments, see Appendix B, “Configuring Dual-NIC Cisco Unified Videoconferencing Solution Deployments”.

Deployments use these connections:

- Tunneled—The normal UDP or TCP ports used for the media or control are not open in the complete path from Desktop Client to Cisco Unified Videoconferencing Desktop Server allowing you to use either a limited UDP port or a TCP port or just HTTP. The media is repacketized to accommodate the open connection; in some instances the media is made compatible with HTTP in order to tunnel through open ports or proxy servers. For the real time media this means:
  - For Desktop Client—SRTP/RTP/UDP traffic is tunneled through TCP or HTTP on port 80 or 443.
  - For streaming—TCP port 7070 or port 80 is used for web access and control (port 80, 443 or 8080).
  - For web access and conference control—TCP port 80, 443 or 8080 is used.
- Untunneled—The normal port ranges of operation for UDP or TCP are opened so that the Desktop Client or Cisco Unified Videoconferencing Desktop Server can communicate without repackaging or redirecting to alternate ports or protocol (UDP to TCP or HTTP).

- Selecting a Deployment, page 1-2
- Selecting a Deployment Topology, page 1-1
- Selecting Components, page 1-3

Selecting a Deployment

To select your deployment, review the list of features different Cisco Unified Videoconferencing Solution deployments provide and determine the deployment that meets your needs.

Table 1-1 Selecting a Deployment

If you want to provide this functionality	Select this deployment
• Group conferencing • Moderating meetings using Desktop Client interface or Cisco Unified Videoconferencing 3500 MCU Conference Control interface • Recording and playback • Sametime Integration • Capacity—support as many calls as a single Cisco Unified Videoconferencing 3500 MCU is capable of supporting	Basic deployment
• Group conferencing • Personal virtual rooms • Multiple Desktop portals • Multiple MCUs • Scalable recording and playback of both public and private recordings • Scheduling and reservation through Desktop Outlook Plug-in or the Cisco Unified Videoconferencing Manager Outlook Add-on • Service preservation • Built-in NAT and Firewall Traversal • Sametime integration • Hosting third-party H.323 and SIP endpoint on Cisco Unified Videoconferencing 3545 EMP	Advanced deployment, including the following topologies • Small Centralized • Large Centralized • Distributed Single-Zone

Selecting a Deployment Topology

- About Cisco Unified Videoconferencing Solution Deployments, page 1-1
- About a Basic Deployment of the Cisco Unified Videoconferencing Solution, page 1-4
- About a Small Centralized Topology of the Cisco Unified Videoconferencing Solution, page 1-6
- About a Large Centralized Topology of the Cisco Unified Videoconferencing Solution, page 1-10
- About Large Distributed Single-zone Deployment of the Cisco Unified Videoconferencing Solution, page 1-12

Selecting Components

Table 1-2 lists components deployed in different deployments.

Table 1-2 Selecting Components

For this deployment	You can deploy these components
Basic	• Cisco Unified Videoconferencing Desktop Server (including the Streaming and Recording Server) • Single Cisco Unified Videoconferencing 3500 Series MCU and Cisco Unified Videoconferencing 3545 EMP or Cisco Unified Videoconferencing 5000 Series MCU • Cisco IOS H.323 Gatekeeper (optional)
Advanced	• Cisco Unified Videoconferencing components: – Cisco Unified Videoconferencing Desktop Server – Streaming Server – Recording Server – Presence Server – Cisco Unified Videoconferencing Manager – Multiple Cisco Unified Videoconferencing 3500 Series MCUs with EMPs and/or Cisco Unified Videoconferencing 5000 Series MCUs – Cisco IOS H.323 Gatekeeper (neighbored) – SIP B2BUA • Third-party components: – Load balancer – SIP Proxy – H.323 gatekeepers • Optional third-party components: – IBM Domino – IBM Sametime Connect – IBM Web Collaboration – Microsoft Server domain – Microsoft Exchange Server – Microsoft Active Directory – Microsoft Office Communications Server (OCS)

About a Basic Deployment of the Cisco Unified Videoconferencing Solution

This is the most basic deployment available if the Cisco Unified Videoconferencing Desktop Server uses a single NIC card. This deployment is particularly attractive for small and medium enterprises having a single main site.

Note If necessary, you can configure a second NIC with a private address for the Cisco Unified Videoconferencing Desktop Server.

This topology contains these solution components:

- Cisco Unified Videoconferencing Manager with the following components activated:
  - Desktop
  - Desktop Streaming Server
  - Desktop Recording Server
  - Internal Gatekeeper (optional)

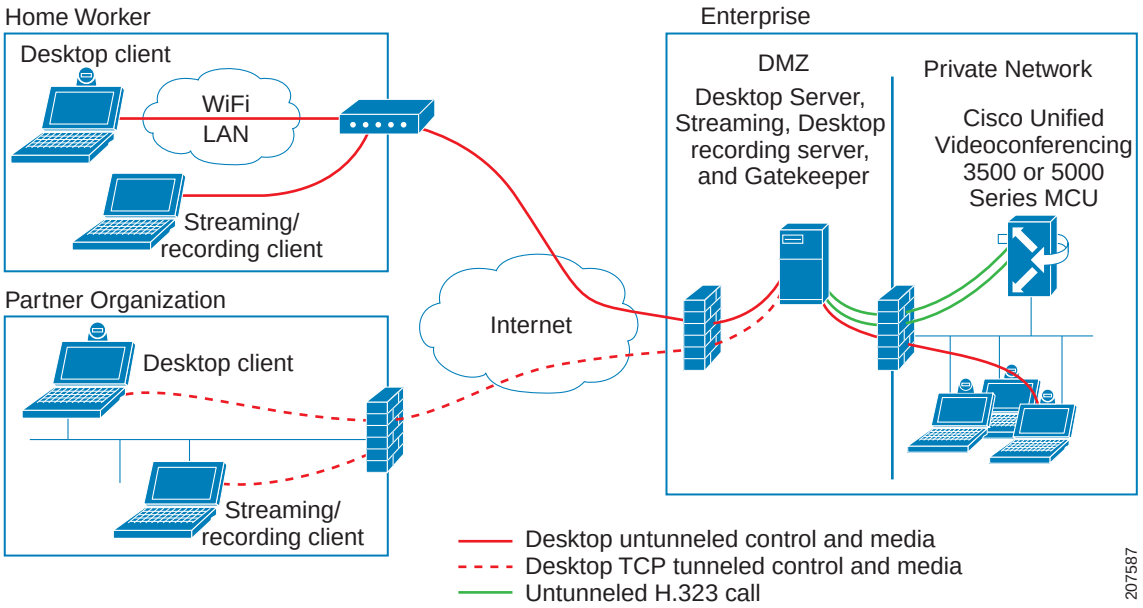
Note All components are installed, but only the above components are required for this type of deployment and only these components are activated.

- Cisco Unified Videoconferencing 3500 MCU or Cisco Unified Videoconferencing 5000 Series MCU

The connection outside the enterprise is handled by the Desktop Client only.

Figure 1-1 shows basic Cisco Unified Videoconferencing Solution deployment.

Figure 1-1 Basic Deployment



Note We recommend to open UDP ports on the firewall for Real Time Transport Protocol for the untunneled connection between the Desktop Client and the Cisco Unified Videoconferencing Desktop Server.

Related Topics

- Basic Deployment Functionality, page 1-5
- Basic Deployment Limitations, page 1-6

Basic Deployment Functionality

This solution supports conference participants belonging to the same enterprise. The deployment allows moderation of meetings using either the Desktop Client interface or the Conference Control interface of the MCU. The Desktop technology supports firewall and NAT traversal for Desktop connection via public networks.

This solution also supports IP dialing to the MCU and the auto-attendant (video IVR) feature. The MCU IP address should be used for IP dialing into the auto-attendant (video IVR) systems.

To enable the video IVR feature for external users, the MCU IP address must be remotely accessible and you must configure the internal and external firewall for H.323 signaling.

The number of desktops and room systems that can attend the same meeting depends on the MCU model and configuration deployed.

To configure a firewall correctly for this deployment, see recommendations described in Configuring Windows Firewall, page A-12.

Basic Deployment Limitations

This topology does not support the resource reservation feature.

The IP dialing for this deployment is only supported inside the private network.When a tunnelled connection is used, the rate of TCP calls is limited to 384 Kbps.

Since the Resource Manager component of the Cisco Unified Videoconferencing Manager is not activated in this topology, features such as virtual rooms, automatic MCU cascading and conference resource reservation are not supported.

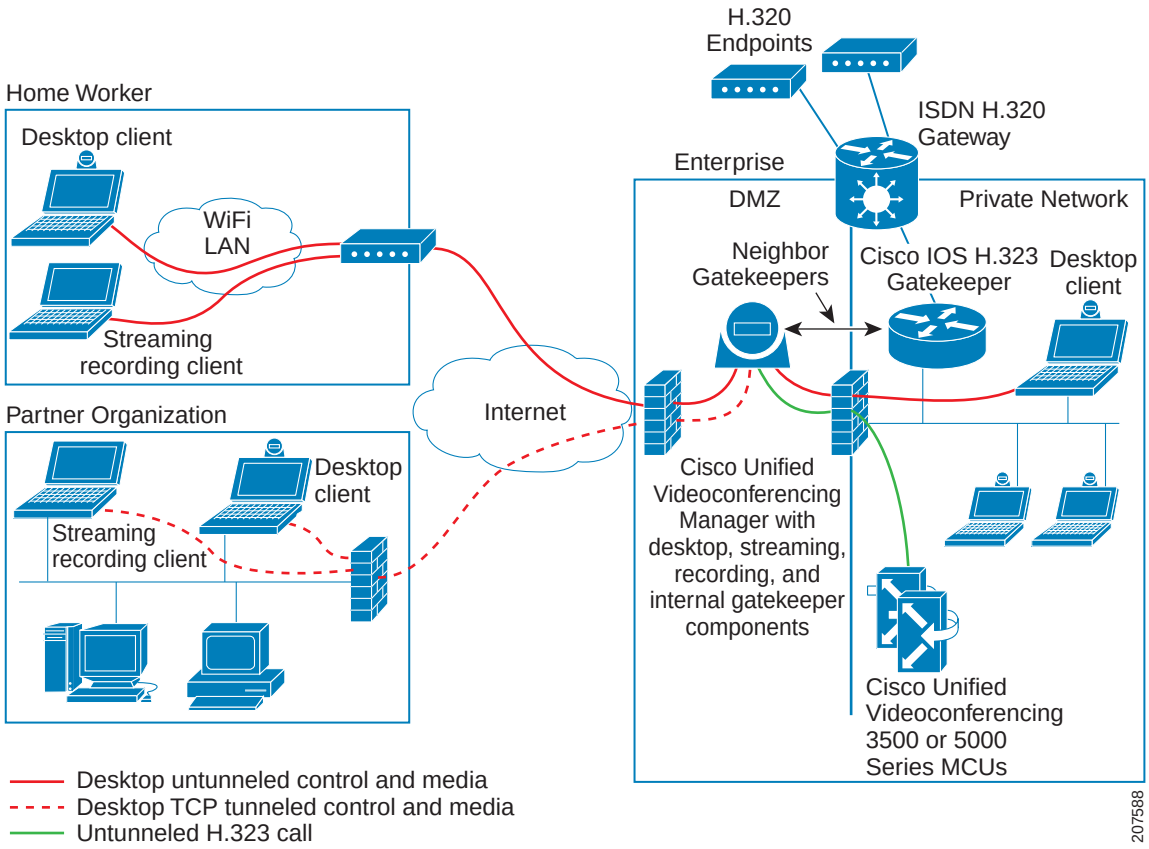
This topology has only one MCU component; therefore, a conference cannot span multiple MCUs. In this case automatic cascading is not possible.

About a Small Centralized Topology of the Cisco Unified Videoconferencing Solution

This deployment suits medium and large networks, and provides this functionality:

- Uses a single Cisco Unified Videoconferencing Desktop Server together with multiple MCU components to connect desktop clients both inside and outside the corporate network.
- Connects room systems inside a corporate network.
- Conferencing solution for ISDN systems on the PSTN network using Cisco Unified Videoconferencing 3500 Series Gateways.
- Uses the Resource Manager component to provide scheduling, resource reservation, virtual MCU scalability across multiple MCUs.
- Support for IP dialing both from inside and outside the enterprise network.
- Support for auto-attendant (video IVR) which allows a participant using an endpoint to hear and view a list of conferences currently running on all MCUs and to join one of them.

Figure 1-2 Small Centralized Deployment



Note We recommend to open UDP ports on the firewall for Real Time Transport Protocol for the untunneled connection between the Desktop Client and the Cisco Unified Videoconferencing Desktop Server.

This deployment typically includes these components:

- Multiple Cisco Unified Videoconferencing 3500 MCU or Cisco Unified Videoconferencing 5000 Series MCU—Located in the firewall-protected private network.
- Cisco Unified Videoconferencing Desktop Server—Located in the firewall-protected DMZ.
- Cisco Unified Videoconferencing Manager—Provides support of Directory Server integration and virtual rooms as well as user management including user authentication. Located in the firewall-protected DMZ. This component can be installed on the same server as Cisco Unified Videoconferencing Desktop Server or Cisco Streaming Server, or on separate dedicated servers for better performance and capacity.
- Cisco IOS H.323 Gatekeeper—Located in the firewall-protected network.
- Room videoconferencing systems
- Cisco Unified Videoconferencing 3500 Series Gateways
- ISDN videoconferencing endpoints on the PSTN/ISDN network

For this deployment, the Desktop and Streaming components of the Cisco Unified Videoconferencing Manager are typically installed on the same server as the Cisco Unified Videoconferencing Manager. Multiple MCUs are located on the private network.

Related Topics

- Small Centralized Deployment Functionality, page 1-8
- Small Centralized Deployment Limitations, page 1-9

Small Centralized Deployment Functionality

The Cisco Unified Videoconferencing Desktop Server resides in the DMZ. The deployment supports:

- Desktop Clients both inside and outside the corporate network
- Room systems inside the corporate network
- Directory Server integration
- Video conference scheduling via web or Microsoft Outlook
- MCU resource reservation for scheduled conferences
- Virtualization of multiple-MCU deployments for seamless scalability
- ISDN systems on the PSTN/ISDN network
- IP dialing from inside the enterprise network
- Auto-attendant (video IVR) which allows to join any current conference.

To configure a firewall correctly for this deployment, see recommendations described in Configuring Windows Firewall, page A-12.

About Using Cisco Unified Videoconferencing 3500 MCUs and Cisco Unified Videoconferencing 5000 Series MCUs in the Same Deployment

In deployments using both Cisco Unified Videoconferencing 3500 MCU and Cisco Unified Videoconferencing 5000 Series MCU, the MCUs are managed by Cisco Unified Videoconferencing Manager.

For consistent user experience and most effective utilization of the resources, we recommend that you define and distinguish between types of services. For example, service prefixes XX on the Cisco Unified Videoconferencing 3500 MCU and service prefixes YY defined on the Cisco Unified Videoconferencing 5000 Series MCU.

These types of services can then be provisioned accordingly to the various user groups in the organization (for example, while one user group receives Cisco Unified Videoconferencing 5000 Series MCU High Definition Services, other user groups receive the Cisco Unified Videoconferencing 3500 MCU Standard Definition Services) or be defined as different service types to different types of meetings (for example, low bandwidth, Standard Definition, Desktop-only meetings using Cisco Unified Videoconferencing 3500 MCU Service, High Bandwidth Desktop and Room-based Systems, requiring HD video, are using Cisco Unified Videoconferencing 5000 Series MCU Service).

When virtual rooms are deployed, each virtual room can be associated to the relevant service prefix, according to the owner's group provisioning and without affecting the dial plan. In this case the same virtual room prefix is used for all users; each user group is associated to the relevant service prefix and therefore to the Cisco Unified Videoconferencing 3500 MCU or Cisco Unified Videoconferencing 5000 Series MCU pool of resources.

Multiple virtual rooms per person can also be defined. Each virtual room is associated to its required service type. For example, one virtual room may be associated to a Cisco Unified Videoconferencing 3500 MCU Service Prefix XX and used for the My Desktop-only standard definition meetings, while another virtual room is associated to a Cisco Unified Videoconferencing 5000 Series MCU Service Prefix YY and used for the My Desktop & Rooms high definition meetings.

Cisco Unified Videoconferencing Manager version 7.1 introduces fallback meeting types, enabling you to configure an automatic fallback from one MCU to another to ensure constant up-time in the event of an MCU failure or lack of resources. This feature allows you to specify one MCU as the default device, like a Cisco Unified Videoconferencing 5000 Series MCU, while a different MCU is defined as the fallback device.

If the MCU fails when a scheduled or ad-hoc meeting is about to start, the system automatically turns to the fallback MCU, allowing the meeting to take place as planned. The dial plan remains unchanged and participants may use the original published meeting number to join.

We recommend using the Cisco Unified Videoconferencing 5000 Series MCU as the main device, and using a Cisco Unified Videoconferencing 3500 MCU as the fallback. This provides the best user experience and high availability when an MCU failure or lack of resources occurs.

The fallback feature can also be used to switch the media used in a call. For example, you can define a fallback from a video-enabled meeting type to an audio-only meeting type.

Note While it is not a recommended approach, cascading the Cisco Unified Videoconferencing 3500 MCU and Cisco Unified Videoconferencing 5000 Series MCU, is possible when performed manually. To perform manual cascading, dial out from a conference running on the MCU belonging to one type to a second conference running on the MCU of other type. Once established, the cascaded conference is seamlessly managed by the latest release of the Cisco Unified Videoconferencing Manager in terms of conference control and moderation capabilities.

In both centralized and distributed topologies of advanced mixed-MCU deployments, the auto attendant feature, is also supported and shows ongoing conferences running on MCUs of both types.

Small Centralized Deployment Limitations

Because all components of Cisco Unified Videoconferencing Manager are installed in a single server in the DMZ, the maximum capacity achievable on supported Cisco Media Convergence Servers (MCS) is 50 simultaneous Desktop client connections and 150 simultaneous live conference streams.

The network must provide sufficient bandwidth between the DMZ and internal network to support up to 250 endpoints, depending on the license.When a tunnelled connection is used, the rate of TCP calls is limited to 384 Kbps.

The network must provide sufficient bandwidth between the DMZ and internal network to support up to 250 endpoints, depending on the license.When a tunnelled connection is used, the rate of TCP calls is limited to 384 Kbps.

To increase scalability by expanding the small centralized deployment, you can install the Streaming and Recording components on separate servers.

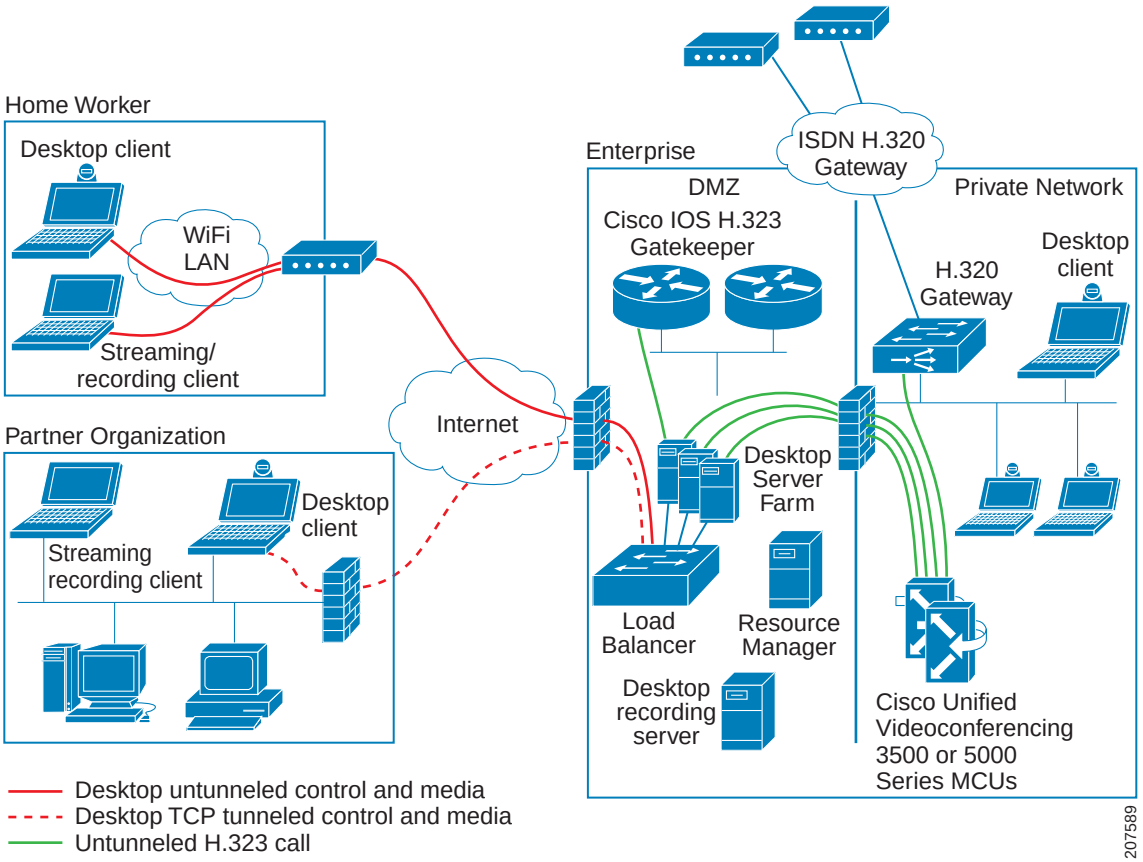
About a Large Centralized Topology of the Cisco Unified Videoconferencing Solution

This deployment suits large enterprises providing:

- Conferencing solution using multiple Cisco Unified Videoconferencing Desktop Servers together with multiple Cisco Unified Videoconferencing 3500 MCU or Cisco Unified Videoconferencing 5000 Series MCU components to provide scalable support of Desktop participants both inside and outside the corporate network.
- Conferencing solution for room systems inside the corporate network using the Internal Gatekeeper.
- Conferencing solution for ISDN systems on the PSTN network using Cisco Unified Videoconferencing 3500 Series Gateways.
- IP dialing from external H.323 endpoints.

Figure 1-3 shows the large centralized Cisco Unified Videoconferencing Solution deployment.

Figure 1-3 Large Centralized Deployment



Note We recommend to open UDP ports on the firewall for Real Time Transport Protocol for the untunneled connection between the Desktop Client and the Cisco Unified Videoconferencing Desktop Server.

This deployment typically includes these components:

- Multiple Cisco Unified Videoconferencing 3500 MCU or Cisco Unified Videoconferencing 5000 Series MCU components—Located in the firewall-protected private network.
- Cisco Unified Videoconferencing SolutionCisco Unified Videoconferencing Manager components:
  - Cisco Unified Videoconferencing Desktop Servers —Multiple servers deployed in the firewall protected DMZ. The load from the Desktop participant connections is evenly distributed between the Desktop Servers by clustering or a load balancer (see Configuring Cisco Unified Videoconferencing Desktop Servers for Scalability and High Availability, page 4-1)
  - In cases where the load balancer is deployed we recommend to configure the load balancing deployment so that Desktop Clients joining the same meeting are routed to the same Cisco Unified Videoconferencing Desktop Server.

Note Additional Cisco Unified Videoconferencing Desktop Servers can be deployed for secure internal access.

  - Desktop Streaming Server—Dedicated server for live streaming audience.
  - Resource and Network Manager Server, including the Internal Gatekeeper—Providing the scheduling, resource reservations, virtualization of multiple MCUs, and network management of videoconferencing infrastructure.
  - Desktop Recording Servers—Located in the firewall-protected DMZ.
- Cisco Unified Videoconferencing 3500 Series Gateway—Located on the firewall-protected private network.
- Room (H.323, SIP, SCCP) videoconferencing endpoints
- ISDN (H.320) videoconferencing endpoints on the PSTN/ISDN network

Note For optimal streaming scalability, we recommend installing the Streaming Server and the Desktop Recording Server components on a separate server. You can also deploy a Streaming Server and a Desktop Recording Server per each Cisco Unified Videoconferencing Desktop Server for enhanced scalability.

Related Topics

- Large Centralized Deployment Functionality, page 1-11
- Large Centralized Deployment Limitations, page 1-12

Large Centralized Deployment Functionality

The deployment supports Desktop participants both inside and outside the corporate network, and room systems inside the corporate network. The deployment also supports ISDN systems on the PSTN/ISDN network. Cisco Unified Videoconferencing Manager provides scheduling, resource reservation, network management, support of Directory Server integration and virtual rooms (reservationless personal videoconferencing IDs).

To configure a firewall correctly for this deployment, see recommendations described in Configuring Windows Firewall, page A-12.

For more information about deploying MCUs of different types in the same deployment, see About Using Cisco Unified Videoconferencing 3500 MCUs and Cisco Unified Videoconferencing 5000 Series MCUs in the Same Deployment, page 1-8.

Large Centralized Deployment Limitations

The deployment requires a load balancer. However, a load balancer is not necessary for using Desktop in streaming mode. The chat and 'raise hand' Desktop participant features do not function properly in deployments with multiple Cisco Unified Videoconferencing Desktop Servers. If multiple Cisco Unified Videoconferencing Desktop Servers are used in the same call, additional MCU ports are used. The IP dialing into auto-attendant (video IVR) systems is supported for internal network H.323 systems only.

To enable the video IVR feature for external users, the MCU and Cisco IOS H.323 Gatekeeper IP addresses must be remotely accessible and you must configure the internal and external firewall for H.323 signaling.

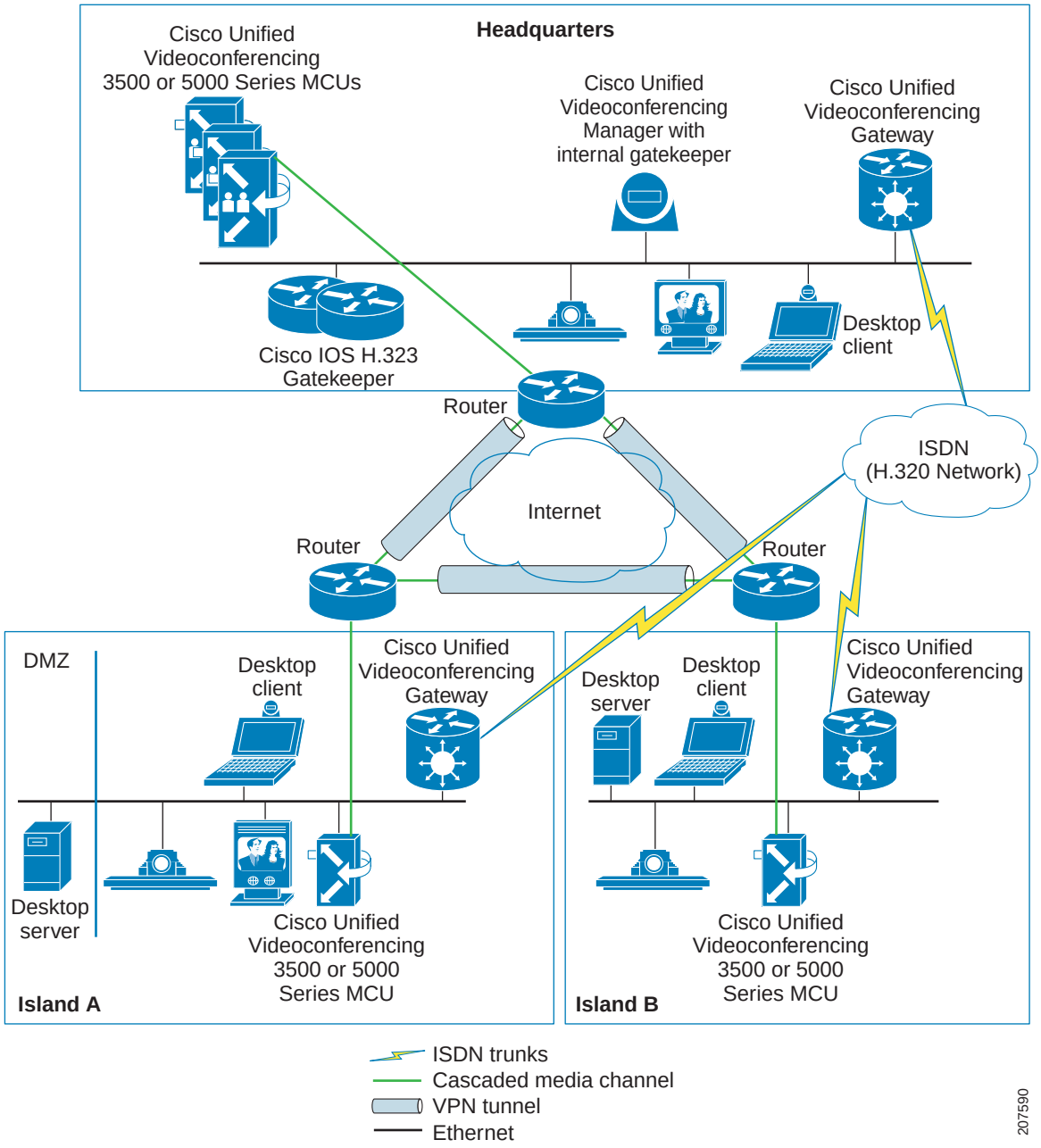
About Large Distributed Single-zone Deployment of the Cisco Unified Videoconferencing Solution

This deployment suits large multi-site enterprises providing:

- Conferencing solution using multiple Cisco Unified Videoconferencing Desktop Servers with multiple Cisco Unified Videoconferencing 3500 MCU/EMP or Cisco Unified Videoconferencing 5000 Series MCU systems for each location to provide scalable Desktop Clients both inside and outside the corporate network.
- Support for multiple Desktop Clients both inside and outside the corporate network, and room systems inside the corporate network.
- Conferencing solution for ISDN systems on the PSTN network using Cisco Unified Videoconferencing 3500 Series Gateway.
- Bandwidth and conferencing resources management solution using Cisco Unified Videoconferencing Manager.
- IP dialing support and enterprise-wide auto-attendant (video IVR).

Figure 1-4 shows the large distributed single-zone Cisco Unified Videoconferencing Solution deployment.

Figure 1-4 Large Distributed Single-Zone Deployment



This deployment includes these components:

- Multiple Cisco Unified Videoconferencing 3500 MCU with EMP or Cisco Unified Videoconferencing 5000 Series MCU—Located on the firewall-protected enterprise network, to support virtual meetings across zones.
- Cisco Unified Videoconferencing Desktop Servers—Located on the firewall-protected enterprise network for enterprise users, or in the DMZ to allow external users to connect. Each branch office is equipped with Cisco Unified Videoconferencing Desktop Servers to provide Desktop Client services coverage to the specific geographical area.

- Cisco Unified Videoconferencing Manager—Located on the firewall-protected enterprise network at the headquarters site. It accesses each Desktop which can be secured with TLS encryption.
- Alternate Cisco IOS H.323 Gatekeeper—Located on the firewall-protected enterprise network at the headquarters site, to route calls to multiple MCUs in different zones.
- Cisco Unified Videoconferencing 3500 Series Gateway—Located on the firewall-protected enterprise network, each branch office is equipped with Cisco Unified Videoconferencing 3500 Series Gateway to provide ISDN room system services coverage to the specific geographical area.
- Internal Enterprise Room systems
- ISDN endpoints on the PSTN/ISDN network
- SIP B2BUA—Routes SIP calls
- Desktop Streaming Servers
- Desktop Recording Servers

Related Topics

- Large Distributed Single-zone Deployment Functionality, page 1-14
- Large Distributed Single-zone Deployment Limitations, page 1-15

Large Distributed Single-zone Deployment Functionality

The large distributed single-zone deployment consists of a headquarters site and several remote sites which are referred to as “islands”. Cisco Unified Videoconferencing Manager situated at the headquarters site is used to manage all deployment components and resources in agreement with the network topology configuration. For example, if a video conference is created on island A, users from island B can join the conference using the island B Cisco Unified Videoconferencing 3500 MCU, because Cisco Unified Videoconferencing Manager can manage cascading between island A MCU and island B MCU, allowing the users to seamlessly join the conference.

Note In multiple-MCU deployments using both Cisco Unified Videoconferencing 3500 MCUs and Cisco Unified Videoconferencing 5000 Series MCUs, Cisco Unified Videoconferencing Manager can manage automatic cascading only between MCUs of the same type. Cascading between MCUs of different types can be achieved by manual cascade. For more information, see About Using Cisco Unified Videoconferencing 3500 MCUs and Cisco Unified Videoconferencing 5000 Series MCUs in the Same Deployment, page 1-8.

While a Desktop conference is created at the Cisco Unified Videoconferencing Desktop Server located on one of the islands, users from any island in the topology can connect to it due to Cisco Unified Videoconferencing Manager resource management.

Cisco Unified Videoconferencing Manager provides support for Directory Server integration and virtual rooms of multi-site enterprises.

This deployment supports up to 250 Desktop Clients per Cisco Unified Videoconferencing Desktop Server.

This deployment assumes that islands are interconnected using a third-party VPN solution. Islands which are connected to unprotected public network, such as Internet, must be protected by a firewall.

Large Distributed Single-zone Deployment Limitations

A single-zone dial plan must be used since this deployment supports only the single H.323 zone topology.

When a tunnelled connection is used, the rate of TCP calls is limited to 384 Kbps.

CHAPTER 2

Installing and Upgrading Components of the Cisco Unified Videoconferencing Solution

This chapter describes Cisco Unified Videoconferencing Solution Server hardware requirements, installation procedures for Cisco Unified Videoconferencing Manager and Cisco Unified Videoconferencing Desktop Server, and upgrade information. The following topics are covered:

- Prerequisites for Installing the Cisco Unified Videoconferencing Solution Components, page 2-2
- About Installing Cisco Unified Videoconferencing Solution Hardware Components, page 2-5
- How to Install Cisco Unified Videoconferencing Solution Software Components, page 2-5
- About Upgrades, page 2-6

Note We recommend that you perform installation procedures in the order described in this chapter.

Prerequisites for Installing the Cisco Unified Videoconferencing Solution Components

Table 2-1 describes the prerequisites for installing Cisco Unified Videoconferencing Solution components.

Table 2-1 Prerequisites for Installing Cisco Unified Videoconferencing Solution Components

For This Component	Do This
Hardware components	Prepare and mount these hardware components: • Cisco Unified Videoconferencing 3500 MCUs and EMPs • Cisco Unified Videoconferencing 3500 Series Gateway • Cisco Media Convergence Server (MCS)
Software components	Verify you have these items: • Desktop product CD-ROM • Desktop license key • Cisco Unified Videoconferencing Manager product CD-ROM • Cisco Unified Videoconferencing Manager permanent license and serial number • Cisco Unified Videoconferencing 3500 MCU and EMP product CD-ROMs • Cisco MCS Server operating system CD-ROM (shipped with Cisco Unified Videoconferencing Manager product CD-ROMs)

Related Topics

- For information about the Cisco Unified Videoconferencing 3500 MCU and Cisco Unified Videoconferencing 3500 Series Gateway, see the User Guides at: http://www.cisco.com/en/US/products/hw/video/ps1870/products_user_guide_list.html.
- For information about the Cisco Unified Videoconferencing 5000 Series MCU, see the User Guides at http://www.cisco.com/en/US/products/ps10767/products_user_guide_list.html and http://www.cisco.com/en/US/products/ps10463/products_user_guide_list.html.
- For more information about Cisco MCS Servers, see Table 2-3 on page 4.
- For information about obtaining appropriate Cisco Unified Videoconferencing Manager and Desktop license keys, see the Cisco Unified Videoconferencing Manager License Fulfillment Instruction at: http://cisco.com/en/US/products/ps7088/prod_installation_guides_list.html.

Cisco Unified Videoconferencing Solution Installation

- Server Preparation, page 2-3
- Providing Sufficient Bandwidth, page 2-3

Server Preparation

You must use either the Cisco MCS 7825, Cisco MCS 7835 or Cisco MCS 7845 RC1 Servers for the Cisco Unified Videoconferencing Manager installation.

Observe these guidelines to prepare a server for the Cisco Unified Videoconferencing Solution installation:

- Use the right duplex configuration on your Ethernet NIC cards. It is essential for optimizing the videoconferencing experience.
- Use 100 Mb full duplex NIC settings for the switch and the Cisco Unified Videoconferencing Solution server.
- If you use a Gigabit NIC and switch, set the duplex setting to auto-sense. Do not use the auto-sense setting if you are not using a Gigabit NIC and switch because auto-sense might cause significant packet loss.
- Use a 32-bit operating system for Cisco Unified Videoconferencing Manager installation. 64-bit operating systems are not supported at this time.
- Verify that the operating system is Windows® 2003 with the latest Service Releases. You can download the Media Convergence Server Operating System software Updates from the Cisco.com Software Download tool at this location:

  http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=268438148.

Providing Sufficient Bandwidth

Cisco Unified Videoconferencing Desktop Server acts as a gateway between the participant personal computers and the Cisco Unified Videoconferencing 3500 MCU. Table 2-2 shows the bandwidth resources required to enable between 10 and 250 users to connect through the system and initiate hundreds of streaming sessions. We recommend that you use statistics provided in Table 2-2 to plan your deployment and NIC card requirements.

Note Use bonded 100 Mbit NICs or a Gigabyte NIC. Default settings are 384 Kbps (interactive), 256 Kbps (streaming).

For each Desktop Client the following traffic is handled by a single Cisco Unified Videoconferencing Desktop Server:

- Desktop Client sends media to Cisco Unified Videoconferencing Desktop Server.
- Cisco Unified Videoconferencing Desktop Server forwards media to Cisco Unified Videoconferencing 3500 MCU.
- Cisco Unified Videoconferencing 3500 MCU returns media to Cisco Unified Videoconferencing Desktop Server.
- Cisco Unified Videoconferencing Desktop Server sends media to Desktop Client.

Therefore, the formula for calculating bandwidth required for interactive session is as follows:

Bandwidth = bandwidth required for one connection × 4 × number of connections

Thus, for a 384 Kbps call there is 1536 Kbps of media going through the Cisco Unified Videoconferencing Desktop Server for each client.

Streaming connections are used to send media from the Cisco Unified Videoconferencing Desktop Server to Desktop Clients. The formula for calculating the bandwidth required for streaming session is as follows:

Bandwidth = bandwidth required for one connection × number of connections

For a high definition call, Cisco Unified Videoconferencing Desktop Server sends 512 Kpbs and receives 1 Mb, which doubles the bandwidth required for the 384 Kbps standard definition call, for which Cisco Unified Videoconferencing Desktop Server sends and receives 384 Kpbs for a total of 768 Kbps. Thus, a high definition call reduces the number of supported interactive connections to 50 percent as shown by Table 2-2 and Table 2-3.

Table 2-2 Required Bandwidth Resources—Standard Definition Connections

Interactive Connections	Streaming Connections	Bandwidth for Interactive Connections (Kbps)	Bandwidth for Streaming Connections (Kbps)	Total Bandwidth (Kbps)
		384	384	
10	30	15360	11520	26880
25	75	38400	28800	57200
50	150	76800	57600	134400
100	300	153600	115200	268800
150	450	230400	172800	N/A (install streaming server on separate computer)
200	600	307200	230400	N/A (install streaming server on separate computer)
250	0	38400	0	N/A (install streaming server on separate computer)

Table 2-3 Required Bandwidth Resources—High Definition Connections

Interactive Connections	Streaming Connections	Bandwidth for Interactive Connections (Kbps)	Bandwidth for Streaming Connections (Kbps)	Total Bandwidth (Kbps)
1		768/1024	384	
5	15	17920	11520	26880
12	36	38400	28800	57200
25	75	76800	57600	134400
50	150	153600	115200	268800
75	225	230400	172800	N/A (install streaming server on separate computer)
100	300	307200	230400	N/A (install streaming server on separate computer)
125	600	38400	0	N/A (install streaming server on separate computer)

Note Using Desktop Clients in HD mode requires larger bandwidth as well as a more powerful Cisco Unified Videoconferencing Desktop Server.

The Recording Server is managed separately. Set the maximum bandwidth for recording playback based on the server hardware capabilities. In deployments where the Recording Server is installed on the same server as the Cisco Unified Videoconferencing Desktop Server, users watching recorded meetings take up Desktop bandwidth which can be used for other purposes, such as meetings. Use the Playback Bandwidth area to configure bandwidth usage for such deployments. Set the Total Bandwidth Allowed value to define a total amount of bandwidth Desktop uses for playing back recorded meetings.

For example, if you set the Total Bandwidth Allowed value to 100 Mbps, Desktop allows a bandwidth of 100 Mbps if one user watches a recording, and a bandwidth of 50 Mbps for each user if two users watch recordings. Set the Minimum Bandwidth required for download value to prevent too many users watching recordings at the same time.

In general, you should not allow a total bandwidth of more than 350 Mbps interactive, streaming and recording connections on the server.

About Installing Cisco Unified Videoconferencing Solution Hardware Components

Install the Cisco Unified Videoconferencing Solution hardware components as described in the corresponding installation manuals supplied on product CD-ROMs.

How to Install Cisco Unified Videoconferencing Solution Software Components

This section describes how to perform installation of Cisco Unified Videoconferencing Solution components and covers the following topics:

- Installing the Resource Manager Component of the Cisco Unified Videoconferencing Manager, page 2-6
- Installing Cisco Unified Videoconferencing Desktop Server, page 2-6

Installing the Resource Manager Component of the Cisco Unified Videoconferencing Manager

Install the Resource Manager component of the Cisco Unified Videoconferencing Manager as described in the *Installation Guide of the Cisco Unified Videoconferencing Manager*.

Installing Cisco Unified Videoconferencing Desktop Server

For deployments of more than 100 users in which streaming is heavily used or for deployments in which port 80 is used for streaming, we recommend that you install the streaming server on a separate server.

The Streaming Server software component of the Cisco Unified Videoconferencing Manager is always installed under C:\Program Files, even if the rest components of Cisco Unified Videoconferencing Desktop Server software are installed at a different location.

For advanced deployments using load balancing devices, install the Cisco Unified Videoconferencing Streaming Server component on all servers.

Install a Cisco Unified Videoconferencing Desktop Server as described in the *Installation Guide for Cisco Unified Videoconferencing Manager.*

About Upgrades

This section provides general information about upgrading Cisco products.

Unless instructed by Cisco Technical Support, the Cisco Unified Videoconferencing components should maintain the software release stated in this section.

Major releases are indicated by the number to the left of first decimal point in the release number. Minor releases are indicated by the number to the right of first decimal point in the release number. Maintenance releases are indicated by the number to the right of the second decimal point in the release number or by the number in parenthesis.

In release number 5.7 (1.0.13) 5 is the major Release, 7 is minor release, and 1.0.13 is maintenance release.

We recommend that upgrades of the Cisco Unified Videoconferencing Solution components are performed in this order:

1. Cisco Unified Videoconferencing Manager, Release 7.1 or greater
2. Desktop components of the Cisco Unified Videoconferencing Manager (including any Streaming components/servers), Release 7.1
3. Cisco Unified Videoconferencing 3500 MCUs (including the MCU modules in both the 3515 Series MCUs and 3545 System), Release 7.1
4. Cisco Unified Videoconferencing 5000 Series MCU Release 7.1
5. Cisco Unified Videoconferencing EMP 3500 modules (including EMP modules in the 3515 Series MCUs and the 3545 System)
6. Cisco Unified Videoconferencing 3500 Series Gateways (including the 3522/3527 Gateway appliances and the 3540 System Gateway modules)

The Desktop Client software is upgraded automatically after the Cisco Unified Videoconferencing Desktop Server is upgraded. For operational information about upgrading a specific component, see the component release notes.

Verify that the release number of the component release notes corresponds to the software release of the component you want to upgrade.

Note If you choose to upgrade by uninstalling and then reinstalling while preserving settings, write the license key in a separate location and use it during the reinstall, since this information is not preserved during uninstallation.

CHAPTER 3

Configuring Cisco Unified Videoconferencing Solution Components

- How to Configure a Cisco Unified Videoconferencing Desktop Server, page 3-1
- How to Configure an MCU, page 3-6
- Configuring Cisco Unified Videoconferencing 3500 Series Gateway, page 3-9
- How to Configure Cisco Unified Videoconferencing Manager, page 3-12
- How to Configure Solution Components for Recording, page 3-16
- Configuring a Gatekeeper, page 3-21
- How to Configure Cisco Unified Videoconferencing Desktop Server to Allow Streaming, page 3-21
- How to Configure Third-Party Equipment, page 3-27

How to Configure a Cisco Unified Videoconferencing Desktop Server

This section describes how to perform a basic Cisco Unified Videoconferencing Desktop Server configuration after the Cisco Unified Videoconferencing Desktop Server is installed. After this configuration is performed, Cisco Unified Videoconferencing Desktop Server is operational and ready to be used for video calls.

- Cisco Unified Videoconferencing Desktop Server, page 3-2
- Cisco Unified Videoconferencing Desktop Recording Server, page 3-2
- Cisco Unified Videoconferencing Desktop Streaming Server, page 3-2
- Configuring Basic Cisco Unified Videoconferencing Desktop Server Settings, page 3-3
- Configuring Meeting Access Instructions, page 3-5

Cisco Unified Videoconferencing Desktop Server

Depending on the topology, there may be more than one Cisco Unified Videoconferencing Desktop Servers used in your deployment.

In deployments where a Cisco Unified Videoconferencing Desktop Server is configured to work with Cisco Unified Videoconferencing Manager and Cisco IOS H.323 Gatekeeper, Desktop continues to function if it loses connection with Cisco Unified Videoconferencing Manager. In this case Desktop switches to a reduced mode and connects to Cisco Unified Videoconferencing 3500 MCU through Cisco IOS H.323 Gatekeeper.

When Desktop is in the reduced mode:

- Users need to dial the full dial plan conference numbers including the zone and the service prefix. For example, 108512345.
- Moderator functions are not available.

Cisco Unified Videoconferencing Desktop Recording Server

Recording can be managed either by a single Cisco Unified Videoconferencing Desktop Server or by multiple Cisco Unified Videoconferencing Desktop Servers.

If a single Cisco Unified Videoconferencing Desktop Server is set to manage recording, only participants connected through that Cisco Unified Videoconferencing Desktop Server can start or stop recording. In this case other Cisco Unified Videoconferencing Desktop Servers in the deployment can be configured to display the list of recordings from the Cisco Unified Videoconferencing Desktop Server configured to manage recording.

If multiple Cisco Unified Videoconferencing Desktop Servers are configured to manage recording, they manage recording independently causing each Desktop portal to display its own list of recordings.

To designate a single Cisco Unified Videoconferencing Desktop Server to manage recording, enable recording on this Cisco Unified Videoconferencing Desktop Server. In this case you must disable recording on other Cisco Unified Videoconferencing Desktop Server in the same deployment, and enable them to allow playback of recordings from an alternate Cisco Unified Videoconferencing Desktop Server in order to display a list of recordings in the portal.

To enable multiple Cisco Unified Videoconferencing Desktop Server for managing recording, enable recording on each Cisco Unified Videoconferencing Desktop Server in this deployment.

Cisco Unified Videoconferencing Desktop Streaming Server

Streaming can be managed either by a single Cisco Unified Videoconferencing Desktop Server or by multiple Cisco Unified Videoconferencing Desktop Servers. If a single Cisco Unified Videoconferencing Desktop Server is set to manage streaming, all other participants are directed to this server. If multiple Cisco Unified Videoconferencing Desktop Servers are configured to manage streaming, they manage streaming independently.

To designate a single Desktop Server to manage streaming, enable streaming on this Cisco Unified Videoconferencing Desktop Server. In this case you must disable streaming on other Cisco Unified Videoconferencing Desktop Servers in the same deployment. However, you can configure those servers to allow watching of webcasts from the Cisco Unified Videoconferencing Desktop Server on which

streaming is enabled. To enable multiple Cisco Unified Videoconferencing Desktop Servers for managing streaming, enable streaming on each Cisco Unified Videoconferencing Desktop Server in this deployment. By default Cisco Unified Videoconferencing Desktop Server uses port 7070 for streaming.

Note **Note** When multiple Cisco Unified Videoconferencing Desktop Servers manage streaming, streaming must be enabled or disabled on each individual Cisco Unified Videoconferencing Desktop Server. For example, if streaming is enabled for a meeting or virtual room, a moderator cannot disable it, because each Cisco Unified Videoconferencing Desktop Server manages streaming independently. If a moderator connected to one Cisco Unified Videoconferencing Desktop Server disables streaming, the other Cisco Unified Videoconferencing Desktop Server still continues to stream, unless it is disabled by its moderator as well.

You can enable and configure multicast streaming to allow unlimited number of simultaneous streaming connections. Multicast streaming in Cisco Unified Videoconferencing Desktop Server is performed without Streaming Server support. During multicast configuration you need to define the Time to Live value—the number of hops of a multicast packet that Cisco Unified Videoconferencing Desktop initiates. Setting this value to 1 means that a multicast packet stays within a local network. The change in the multicast streaming configuration applies only to meetings created after the change takes place; the change does not effect meetings in progress.

Obtain the internal IP address range of accessible Cisco Unified Videoconferencing Desktop Clients to define clients that will be able to watch multicasts.

Configuring Basic Cisco Unified Videoconferencing Desktop Server Settings

This section describes how to configure basic settings after Cisco Unified Videoconferencing Desktop Server is installed and the Desktop Administrator web user interface opens in the configuration wizard mode.

Before You Begin

If you configure multicast streaming:

- Ensure multicast is enabled on the deployment routers and firewalls.
- Verify the number of packet hops to correctly define the Time to Live value.
- Obtain the internal IP address range of accessible Desktop Clients to define clients that will be able to watch multicasts.

Procedure

Step 1 Access the Cisco Unified Videoconferencing Desktop Server Administration interface using the following URL: *http://<ip_address:port>cuvm/admin*.

Step 2 Enter your user name and password.

Note The default user name and password are both “admin”.

The configuration wizard welcome page opens.

Step 3 Select **Next** to begin the configuration wizard.

The Server page opens. Configure servers used in your deployment.

Step 4 To configure a basic deployment, perform these steps:

a. Select **Basic** from the deployment list.

b. Enter the MCU IP address.

c. Enter a user name and password for accessing the MCU Administration web user interface.

d. Re-enter the password in the Confirm field.

The default user name is “admin”. There is no default password for Cisco Unified Videoconferencing 3500 MCU Release 5.x; for Cisco Unified Videoconferencing 5000 Series MCU Release 7.x the default password is “password”.

e. If Cisco Unified Videoconferencing Desktop Server is configured with multiple IP addresses, select the relevant address from the Desktop Network Interface list.

f. To enable recording, select the **Recording** check box, and then enter the Recording Server address.

g. To enable streaming, select the **Streaming** check box, and then enter the Cisco Unified Videoconferencing Streaming Server address.

Step 5 To configure an advanced deployment, perform these steps:

a. Select **Advanced** from the deployment list.

b. Enter the address of Cisco Unified Videoconferencing Manager.

c. If the Cisco Unified Videoconferencing Desktop Server is configured with multiple IP addresses, select the relevant address from the Desktop Network Interface list.

d. Enter IP address of the gatekeeper.

e. Enter the source H.323 ID of the Desktop Server, which matches the H.323 ID configured in the Cisco Unified Videoconferencing Manager for this Cisco Unified Videoconferencing Desktop Server.

f. To enable recording, select the **Recording** check box, and then enter the Recording Server address.

g. To enable streaming, select the **Streaming** check box, and then enter the Streaming Server address.

Step 6 Select **Next**.

The **Settings** tab is displayed.

Step 7 Select **Finish**. The Desktop Status page opens.

Step 8 Verify that all four types of servers are connected.

Note The light next to each link indicates whether or not the connection to the target server or registration with the Gatekeeper is successful. When the light is red, a tooltip containing error details is available. Select the red light to view further error information.

Step 9 If you installed and configured the Desktop Recording Server, select the **Recording Status** tab, and verify that the Desktop Recording Server is connected.

Note The light next to each link indicates whether or not the connection to the server is successful. When the light is red, a tooltip containing error details is available. Select the red light to view further error information.

Related Topics

- Configuring Streaming for Playback Using the UDP Connection, page 3-24

Configuring Meeting Access Instructions

This section describes how to view the default instructions for joining a meeting that the Cisco Unified Videoconferencing Desktop Server Outlook add-on sends to invitees, and how to modify the contents of these email invitations.

Procedure

Step 1 Select **Messages and Invitations** in the sidebar.

Step 2 Select the **Invitations** tab.

The default instructions for accessing the meeting from a desktop, phone or video conferencing device appear on the screen.

Step 3 In the **Desktop Access** section:

- Select **Meeting URL** to insert a link to the meeting.
- Select **Client Installation** to insert a link used to ensure that the Desktop Client is installed and up-to-date.

  If you have multiple Cisco Unified Videoconferencing Desktop Servers and want participants to know about them, insert link information for each of them into each Desktop e-mail configuration. For example, if you have one Desktop in Europe, one in Asia, and another in the US, you could place the following information in your e-mail:

  “From Europe, connect to http://europe.server.com/cuvm?ID=1234&autojoin

  From Asia, connect to http://asia.server.com/cuvm?ID=1234&autojoin

  From the US, connect to http://us.server.com/cuvm?ID=1234&autojoin.”

  The automatically inserted server address is the Desktop FQDN specified during installation.

Step 4 In the Phone Access area, select **E.164** to insert the required E.164 alias.

Step 5 In the Video-Conference Device Access area, select **E.164** to insert the required E.164 alias.

Step 6 Select **OK** or **Apply**.

Restricting H.323 Ports between Cisco Unified Videoconferencing Desktop Server and MCU

Perform these steps to limit the H.323 TCP ports between the Cisco Unified Videoconferencing Desktop Server and the MCU to a predefined port range.

Procedure

Step 1 Navigate to this location:

<CUVCDINSTALLDIR>\Confsrv

where <CUVCDINSTALLDIR> is the default installation directory.

Step 2 Locate the ConfSrv directory.

Step 3 Edit config.val.

Step 4 Locate the [1 system] section.

Step 5 Insert an empty line in that section.

Step 6 Add the words “2 portFrom =”.

Step 7 Enter the lowest port number in the range of available ports.

Step 8 Insert another empty line in that section.

Step 9 Add the words “2 portTo =”.

Step 10 Enter the highest port number in the range of available ports.

Step 11 Save the file.

Step 12 Restart the service "Cisco Unified Videoconferencing Desktop - Conference Server".

How to Configure an MCU

- Performing Basic Configuration of Cisco Unified Videoconferencing 3500 MCU, page 3-6
- Performing Basic Configuration of the Cisco Unified Videoconferencing 5000 Series MCU, page 3-7
- Configuring Auto-Attendant Feature in Multiple-MCU Deployments, page 3-8

Performing Basic Configuration of Cisco Unified Videoconferencing 3500 MCU

Procedure

Step 1 Access the MCU Administration web interface.

Step 2 Configure an IP address of the MCU:

a. If using Cisco Unified Videoconferencing 3545 MCU, select **Board** on the sidebar.

b. If using Cisco Unified Videoconferencing 3515 MCU, select **Device** on the sidebar.

c. Perform any of these steps:

- Enter the IP address you want to assign to the MCU in the IP Address field.
- Enter the IP address of the router you want the MCU to use in the Router IP field.
- Enter the IP address of the subnet mask you want the MCU to use in the Subnet Mask field.

Step 3 Select **MCU** on the sidebar.

Step 4 Verify that the EMP modules appear in the Media Processing tab.

Step 5 Select **H.323** in the Protocols tab.

Step 6 Enter the IP address in the Gatekeeper Address field.

If you use Cisco Unified Videoconferencing Manager as your meeting control server, enter the Cisco Unified Videoconferencing Manager IP address in the Gatekeeper address field so that the MCU uses the Cisco Unified Videoconferencing Manager internal gatekeeper.

Step 7 Select **Upload**.

Step 8 To enable High Definition Continuous Presence conferences, perform the following steps:

Note Enabling High Definition Continuous Presence conferences reduces the MCU capacity.

a. Select **Basics** in the Settings tab.

b. Select **Enable High Definition Continuous Presence**.

c. Select **Upload**.

d. Double-click a service in the Services tab to use for High Definition Continuous Presence conferences.

Note We recommend that you use the preconfigured service 81 HD/SD Continuous Presence.

e. Select **720p** from the Support image size up to list, in the Automatic Service Definition window.

f. Select **Upload**.

Note Configuring the MCU for H.235 (secure video) is not supported by Cisco Unified Videoconferencing Desktop Server.

Performing Basic Configuration of the Cisco Unified Videoconferencing 5000 Series MCU

You can configure the protocol settings of an H.323 gatekeeper to set how the Cisco Unified Videoconferencing 5000 Series MCU and the gatekeeper interact.

Warning **Changing gatekeeper settings does not reset the MCU, but might disconnect active calls.**

Procedure

Step 1 Select **Configuration**.

Step 2 Select **Protocols**.

Step 3 Locate the H.323 section.

Step 4 Select **H.323** to enable the MCU to operate with the H.323 protocol.

Step 5 Enter the IP address and port number for the gatekeeper.

The default port is 1719.

Step 6 Select **Apply**.

Configuring Auto-Attendant Feature in Multiple-MCU Deployments

Auto-attendant feature allows users to dial into the Cisco conferencing system using a global auto-attendant session number which is a system-wide prefix allowing users to connect to an auto-attendant session. This prefix is configured via Cisco Unified Videoconferencing Manager which is used to moderate conferencing in multiple-MCU deployments. Once the auto-attendant session number is configured, the MCU auto-attendance (IVR) mechanism is managed by Cisco Unified Videoconferencing Manager.

Note The auto-attendant session is referred to as "IVR session" in the *User Guide for Cisco Unified Videoconferencing 3500 MCU*.

Configuring an auto-attendant session is performed in two steps:

1. Via the MCU Administrator interface, a new service is created and configured to function as an Cisco Unified Videoconferencing Manager meeting type.
2. Via the Cisco Unified Videoconferencing Manager Administrator interface, the auto-attendant session number is assigned to the service created in the MCU.

After this configuration is performed, an auto-attendant session is created in accordance with the configured service every time a user dials the auto-attendant session number configured in Cisco Unified Videoconferencing Manager.

To dial into the auto-attendant (video IVR) using direct IP dialing, users dial the IP address of the Cisco IOS H.323 Gatekeeper.

Configuring Auto-Attendant Feature on Cisco Unified Videoconferencing 3500 Series MCU

Procedure

Step 1 Access the MCU Administration web interface.

Step 2 Select **MCU** in the sidebar.

Step 3 Select the **Services** tab.

Step 4 Select **Add**.

Step 5 Define the new service parameters in the Automatic Service Definition dialog box:

- Service prefix
- Service description
- Service type—HD/SD Continuous Presence
- Max call rate—Default value of 2048Kbps
- Support image size up to—4CIF
- Clear the **Support presentation view** check box.

Step 6 Select **Advanced Video Settings**.

Step 7 Move the H.263 video codec to the top of the list in the Advanced Video Settings dialog box to assign the highest priority to it.

Step 8 Select **OK**.

Step 9 Select **Upload**.

Configuring Auto-Attendant Feature on Cisco Unified Videoconferencing 5000 Series MCU

Procedure

Step 1 Access the MCU Administration web interface.

Step 2 Select **Configuration**.

Step 3 Select **Conferences**.

Step 4 Locate the Conference Control section.

Step 5 Select **Enable auto attendant**.

Step 6 Enter an auto-attendant number.

Use this option if the MCU is already registered to an H.323 gatekeeper or SIP registrar.

Step 7 (Optional) Select **Prompt for conference PIN during conference creation** if you want the MCU to prompt users for a PIN when accessing a conference using this auto-attendant number.

Step 8 Select **Apply**.

Configuring Cisco Unified Videoconferencing 3500 Series Gateway

Configure gateways in your network to enable PSTN/ISDN/mobile terminals to join a meeting. Resource Manager uses the gateway information to provide proper dialing information for meeting participants, and to dial out to terminals to invite them to meetings. Resource Manager also manages gateway resources to allow successful call scheduling using network gateways.

When you add a gateway, settings in Resource Manager must be consistent with the actual gateway configuration. We recommend the following:

- If you make changes to the gateway, maintain the auto-attendant (video IVR) and DID numbers in the Resource Manager.
- To ensure that there are no gateway ports available for scheduled and ad-hoc calls, maintain capacity information.

Procedure

Step 1 Select **Resource Management** in the sidebar menu.

Step 2 Select **Gateway**.

Step 3 Select the link in the Name column for the gateway you require, or select **Add** to create a new gateway profile.

Step 4 Enter the name of the gateway in the **Name** field.

Step 5 Select a gateway model and enter an IP address in the relevant fields.

Note If multiple gateways are pooled together in a local network with the same access phone number, then you can enter multiple IP addresses in the IP Address field to indicate gateways in the gateway pool. IP addresses are separated by a colon (:).

Step 6 From the **Registered To** list, select the gatekeeper to which the gateway is registered.

Step 7 From the **Location** list, select the device island to which the MCU belongs.

The Location field is visible only when the IP Topology tab is activated in the Resource Manager Configuration Tool under System Configuration > UI Settings.

Step 8 Enter the bandwidth for the gateway or gateway pool. For example, for an E1 line, the bandwidth should be 30 B-channels (3940 Kbps).

Step 9 Indicate in the **Working Mode** field whether the gateway operates in auto-attendant (IVR) or DID mode.

Resource Manager works with the gateway in DID mode so that meeting participants can easily dial into a meeting. You can assign a range of DID numbers to the gateway. These numbers can be assigned to individual dial-in terminals (endpoints). If you dial one of the assigned DID numbers, you are automatically added to the meeting that the DID number is associated with. Only one terminal can dial a DID number at any given time.

If you configure the gateway in DID mode and set a DID number in the Telephone Number field, when a terminal dials this DID number Resource Manager routes the call to the appropriate meeting based on the terminal number. If no associated meeting is found, then the dial-in call is routed back to the gateway for an IVR session. After entering the meeting ID using the IVR, the terminal is permitted to join the meeting.

Step 10 Enter a gateway phone number:

a. Enter a description of the phone number for the gateway in the **Description** field.

b. Enter the numeric prefix required to make an international long distance call in the **International Access Code field**.

c. Enter the numeric prefix required to make a long distance call in the **Domestic Long Distance Prefix** field.

d. Enter the country code for the gateway phone number in the **Country Code** field.

The Resource Manager adds the country code prefix when dial-out is performed from this gateway to a terminal located in a different country.

If **Allow Out of Area Calls** is not checked, only endpoints with the same area code as the gateway are allowed to reach the Resource Manager via the gateway.

If you select **Allow Out of Area Calls**, the gateway accepts incoming calls to the Resource Manager from terminals with a different area code than that of the gateway.

e. Enter the domestic area code of the gateway number in the **Area Code** field.

f. Specify a local telephone number to assign to the specific port in the **Telephone Number** field.

g. Enter a number in the **To access an outside line for local calls, dial** field for a gateway with no direct access to an outside line for local calls.

h. Enter a number in the **To access an outside line for long distance calls, dial** field, for a gateway with no direct access to an outside line for long distance calls.

i. Assign the ISDN device island that the gateway or gateway pool belongs to. If the **ISDN Topology** is hidden, the **ISDN device island** field is also hidden.

Step 11 Define the DID range.

If DID is selected in the **Working Mode** field, define the DID range for the gateway or gateway pool.

Step 12 Select **Add Service** to add or modify the gateway service.

Note If you select **Restricted Mode** in the Bandwidth section, 56 appears in the Kbps list. Multiples of 56 Kbps are used instead of multiples of 64. The Resource Manager does not support gateway services whose bandwidth is set to “auto” since the Resource Manager needs the specific bandwidth to perform resource reservation. If there is a gateway service with “auto” bandwidth, when you configure this service in the Resource Manager, select a bandwidth value to best approximate the average bandwidth endpoints use when dialing that service.

Step 13 Set the Advanced Settings:

a. Set the gateway port used for signaling in the **Signaling Port** field. By default, this field is left blank and the signaling port is negotiated dynamically on the fly.

b. Set the SNMP community name required by the Resource Manager to communicate with the gateway in the **SNMP Get/Set Community** fields.

c. Select **Dial-in Only** to mark the gateway for use only with terminals that users dial into.

Step 14 Select **OK** to save your changes.

How to Configure Cisco Unified Videoconferencing Manager

- Performing Basic Cisco Unified Videoconferencing Manager Configuration, page 3-12
- Configuring an Auto-Attendant Session, page 3-15

Performing Basic Cisco Unified Videoconferencing Manager Configuration

During this procedure you configure the LDAP server that you want Cisco Unified Videoconferencing Manager to work with. As a result, you cannot add new users using the Cisco Unified Videoconferencing Manager interface. Instead you need to configure new users in AD and synchronize AD with Cisco Unified Videoconferencing Manager; then you should be able to see added users in Cisco Unified Videoconferencing Manager.

Procedure

Step 1 Access the Cisco Unified Videoconferencing Manager Administration web interface.

Note For a standard installation, the URL format is http://<server address>:8080.

Step 2 Use the following procedure to define the LDAP you want to work with:

a. Select **Advanced Settings** in the sidebar menu.

b. Select **LDAP Configurations**.

c. Select **Add** to add a new LDAP server, or select the required LDAP server entry to modify an existing LDAP server.

d. Select the type of LDAP server to connect Resource Manager to in the Directory Server Type field.

e. Enter the directory server domain or directory server URL in the **Domain/URL** field.

f. Enter the directory server login ID and password in the relevant fields.

Note The user account needs to have read access to all user accounts that you want to synchronize to the Resource Manager. This user account does not have to be part of the search base.

g. Enter search strings in the **LDAP Search Base** field.

Examples of search conditions are “ou” and “cn”.

h. In the **Advanced** section, assign LDAP users to different user roles in Resource Manager by assigning an LDAP group to a specific Resource Manager user role.

The following user types are available:

- Organization Administrator
- Meeting Operator
- Meeting Organizer
- Regular User
- Default User Type

Note By default, all users are assigned the Meeting Organizer user role.

i. Enter the name of an ADS user group in the **Selected Groups** field, or select the **Select** button in each row to map an ADS user group to each Resource Manager default user type.

   For example, to assign all users in the ADS Organization Administrator user group to the Resource Manager Organization Administrator user role, type "Organization Administrator" in the **Selected Groups** field next to the Organization Administrator user type.

   You can assign multiple ADS user groups to each Resource Manager user role.

   Resource Manager maps all users that are not assigned to any listed Resource Manager user role to the user role specified in the Default User Type field.

   To instruct Resource Manager not to download users that are not assigned to any listed Resource Manager user role, set the Default User Type field to **Don't download**.

j. Select the **Virtual Room Number** check box to create a virtual room for all LDAP users.

k. Select a parameter that you want to use as the virtual room number.

   By default, the telephoneNumber parameter is used since everyone within an organization should have a unique telephone number.

   The resulting virtual room is the concatenation of the Resource Manager Meeting ID prefix and the LDAP field that is used for generating the virtual room number.

   The default Cisco Unified Videoconferencing Manager Meeting ID prefix is 6. If it does not suit the organization dial plan, it can be changed. For operational information, see "Configuring the Cisco Unified Videoconferencing Manager Prefix" section on page -127.

l. To download a user profile from an LDAP server, define the following properties for that user on the LDAP server:

   - User ID and password
   - First name or last name
   - E-mail address
   - Belongs to OU
   - Belongs to a group (if you want to assign a user role based on group)

m. From the **Update Frequency** list select an option to define if and how often the Cisco Unified Videoconferencing Manager updates the LDAP server settings.

n. Select **OK**.

Step 3 On the sidebar, select **User Management**, select the **Users** tab, and then select **Update**. The list of users is displayed.

Note The user database is updated according to advanced settings configured on the LDAP Configurations tab.

Step 4 Verify that connection to the gatekeeper is successful:

a. On the sidebar, select **Resource Management**.

b. Select the **Gatekeeper/SIP server** tab.

c. Verify that all connections are successful.

Step 5 Add MCUs:

a. Select the **MCU** tab, and select **Add**.

b. In the New MCU window, enter data and select **OK**.

c. Verify that all connections are successful and the status is Online. For more information, refer to the *Configuration Guide for Cisco Unified Videoconferencing Manager*.

Step 6 Add gateways:

a. Select the **Gateway** tab, and select **Add**.

b. In the New Gateway window, enter data and select **OK**. For operational information about adding a gateway, refer to the *Configuration Guide for Cisco Unified Videoconferencing Manager*.

Step 7 Configure the predefined Cisco Unified Videoconferencing Desktop Server:

a. Select **Resource Management**.

b. Select the Desktop tab.

c. Select the "Local Desktop Server" link in the **Name** column.

d. Enter the IP address of the Desktop in the relevant fields.

e. In the **Web Access URL** field, change the URL to the public address (FQDN) of your Cisco Unified Videoconferencing Desktop Server, configured on the Servers tab of the Cisco Unified Videoconferencing Desktop Server Administrator interface.

f. Enter the value configured in "How to Configure a Cisco Unified Videoconferencing Desktop Server" section on page 3-1 in the **H.323 ID** field.

g. Select **OK**.

Step 8 Add terminals if necessary. For operational information about adding terminals, refer to the *Configuration Guide for Cisco Unified Videoconferencing Manager*.

Step 9 If the LDAP server configuration needs to be changed, perform this configuration as described in Step 2.

Step 10 Download services:

a. On the sidebar, select **Meeting Types**.

b. Select the **Active Meeting Types** tab.

c. Select **Download**.

d. Verify that services are displayed on the Active Meeting Types tab.

e. Select **OK**.

Step 11 Assign a meeting type to a user virtual room using the Cisco Unified Videoconferencing Manager Administration interface:

a. On the sidebar, select **User Management**.

b. Select the **Users** tab.

c. Select a user.

d. On the User Profile page, select **Virtual Room Settings**.

e. Select **Add**.

f. Enter information and select **OK**.

or

Step 12 Assign a meeting type to a user virtual room using Desktop Client:

a. In an internet browser, enter the Cisco Unified Videoconferencing Desktop Server URL.

b. Without entering your user name and password, select **Virtual Room Settings**.

The Virtual room settings page is displayed.

c. Enter information in the fields.

Note From the **Meeting Type** list, select the meeting type associated with the virtual room.

d. Select **OK**.

Step 13 Update the Cisco Unified Videoconferencing Manager license:

a. Select **Start > Programs > Cisco Unified Videoconferencing Manager > Update License**.

b. Enter the license key and the supplied serial number. For more information about obtaining a license key, refer to the *Installation Guide for Cisco Unified Videoconferencing Manager*.

c. Select **Update**.

Configuring an Auto-Attendant Session

This section describes the configuration you need to perform for deployments using Cisco Unified Videoconferencing Manager for conference moderation.

During this procedure an MCU service, referred to as a meeting type in the Cisco Unified Videoconferencing Manager Administrator interface, is assigned for connecting to the auto-attendant (IVR) session.

Procedure

Step 1 Select **Meeting Types** in the sidebar menu.

Step 2 Select **Active Meeting Types**.

Step 3 Select the name of the service you want to use for entry to the IVR.

Note This service should be preconfigured via the Cisco Unified Videoconferencing 3500 MCU Administrator interface.

Step 4 Select **Use in Auto Attendance session**.

Step 5 Enter a number in the Auto attendance session number field.

Verify that this number does not begin with any MCU or Gateway service or Cisco IOS H.323 Gatekeeper zone prefix, or is the same as the number of an IP terminal.

Step 6 Select **OK** to save your changes.

The designated service is marked with an icon in the Name column of the Active Meeting Types screen.

Related Topics

- Configuring Auto-Attendant Feature in Multiple-MCU Deployments, page 3-8
- Performing Basic Cisco Unified Videoconferencing Manager Configuration, page 3-12

How to Configure Solution Components for Recording

Cisco Unified Videoconferencing Desktop allows users to record meetings and to view recorded meetings. A recording includes all media types: the audio, video and presentation. Servers used for recording meetings must have a recording license installed on them.

Cisco Unified Videoconferencing Desktop supports up to 10 simultaneous recordings.

If you did not provide the Recording Server license key during Cisco Unified Videoconferencing Desktop Server installation, you still have a default evaluation license allowing to record one meeting at a time; each recording duration is limited to five minutes.

This section describes how to configure Cisco Unified Videoconferencing Solution components to enable and support the Desktop recording feature.

- Configuring Cisco Unified Videoconferencing Desktop Server for Recording, page 3-16
- Configuring Cisco Unified Videoconferencing Manager for Recording, page 3-19

Configuring Cisco Unified Videoconferencing Desktop Server for Recording

- Desktop Recording Server Connection, page 3-16
- Configuring This Cisco Unified Videoconferencing Desktop Server to Manage Recording, page 3-17
- Configuring an Alternate Cisco Unified Videoconferencing Desktop Server to Manage Recording, page 3-19

Desktop Recording Server Connection

This section describes how to configure Desktop Recording Server settings. Recording can be managed either by a single Cisco Unified Videoconferencing Desktop Server or by multiple Cisco Unified Videoconferencing Desktop Servers.

If a single Cisco Unified Videoconferencing Desktop Server is set to manage recording, only participants connected through that Cisco Unified Videoconferencing Desktop Server can start or stop recording. In this case other Cisco Unified Videoconferencing Desktop Servers in the deployment can be configured to display the list of recordings from the Cisco Unified Videoconferencing Desktop Server configured to manage recording.

If multiple Cisco Unified Videoconferencing Desktop Servers are configured to manage recording, they manage recording independently causing each Desktop portal to display its own list of recordings.

To designate a single Cisco Unified Videoconferencing Desktop Server to manage recording, enable recording on this Cisco Unified Videoconferencing Desktop Server. In this case you must disable recording on other Cisco Unified Videoconferencing Desktop Server in the same deployment, and enable them to allow playback of recordings from an alternate Cisco Unified Videoconferencing Desktop Server in order to display a list of recordings in the portal.

To enable multiple Cisco Unified Videoconferencing Desktop Server for managing recording, enable recording on each Cisco Unified Videoconferencing Desktop Server in this deployment.

Configuring This Cisco Unified Videoconferencing Desktop Server to Manage Recording

The public address you define during this procedure performs a similar role to the public address defined for the Desktop Server. If the Desktop Recording Server resides behind a NAT, the clients may not resolve the Desktop Recording Server IP address. In this case the clients use the public address to connect to the Desktop Recording Server.

If Cisco Unified Videoconferencing Manager is configured to work with the Desktop Server in advanced deployments, recording policies configured on Cisco Unified Videoconferencing Manager determine whether users are allowed to record meetings or not. However, for basic deployments you need to define the recording policy on Cisco Unified Videoconferencing Desktop Server by enabling the recording option for Desktop users.

You also define the following parameters during this configuration:

- Video size and Recording bit rate—These parameters are used to control the quality of recordings.

  Setting the recording bit rate to a value lower than 256 Kbps can affect the quality and frame rate of the H.239 Data in the live connection and streaming modes.

- Maximum Recording Duration—The value set for this parameter controls maximum allowed duration for any recording.
- Send tone periodically during recording—This parameter defines the frequency of the sound signal played during a recording which serves to remind users that their meeting is being recorded.

In deployments where the Recording Server is installed on the same server as the Cisco Unified Videoconferencing Desktop Server, users watching recorded meetings take up Desktop bandwidth which can be used for other purposes, such as meetings. Use the Playback Bandwidth area to configure bandwidth usage for such deployments. Set the Total Bandwidth Allowed value to define a total amount of bandwidth Desktop uses for playing back recorded meetings. For example, if you set the Total Bandwidth Allowed value to 100 Mb/s, then Desktop allows 100 Mb/s bandwidth if one user watches a recording and 50 Mb/s bandwidth for each user if two users watch recordings. You need to set the Minimum Bandwidth required for download value to prevent too many users watching recordings at the same time.

You can use the Cisco Unified Videoconferencing Manager to automatically record either a virtual room or a scheduled meeting when the meeting begins.

If the deployment in use comprises multiple Cisco Unified Videoconferencing Desktop Servers, automatic recording is performed on all Cisco Unified Videoconferencing Desktop Servers and several identical recordings are created. In this case we recommend that you allow one of the Cisco Unified Videoconferencing Desktop Servers to perform automatic recording, while disabling the Cisco Unified Videoconferencing 3500 Series MCU automatic recording feature on the rest of the Cisco Unified Videoconferencing Desktop Servers in the deployment. The procedure in this section describes how to disable the automatic recording feature on a Cisco Unified Videoconferencing Desktop Server.

When you enable high definition recording in deployments using Cisco Unified Videoconferencing 3545 MCU, Cisco Unified Videoconferencing Desktop Server starts recording in high definition. If the attempt to record in high definition fails, the Cisco Unified Videoconferencing Desktop Server automatically switches to standard definition and continues recording.

Before You Begin

- Navigate to the Cisco Unified Videoconferencing Desktop Server Administration web user interface.
- Select **Deployment** in the sidebar, and verify that the **Recording** check box is selected.

Procedure

Step 1 Verify that the Recording Server address is configured correctly:

a. Select **Status** in the sidebar.

b. Select the **Recording Status** tab.

c. Verify that the IP address in the Recording Server Address field is correct.

Step 2 Select **Recording** in the sidebar.

The Settings tab is displayed.

Step 3 To configure standard definition recording, select a value from the Maximum Bit Rate list under Standard Definition.

Step 4 To configure high definition recording, perform the following.

a. Select the **High Definition** check box.

b. Select a value from the **Maximum Bit Rate** list under **High Definition**.

Step 5 Enter a value in the **Maximum Recording Duration** field.

Step 6 Enter a value in the **Total Bandwidth Allowed** field.

Step 7 Enter a value in the **Minimum Bandwidth** required for download field.

Step 8 From the **Send tone periodically during recording** list, choose an option.

Step 9 To disable automatic recording feature, clear the **Allow virtual rooms and scheduled meetings to be recorded automatically** check box.

Step 10 For basic deployments, select the **Allow meeting participants to record** check box to enable recording for Desktop users.

For advanced deployments, you cannot modify this setting in Desktop, since Cisco Unified Videoconferencing Manager controls the recording policies.

Step 11 In the **Public Address** field, enter a FQDN.

We recommend that you use a FQDN that clients can resolve.

Step 12 Enter the HTTP port.

This port is used by clients to access the recording.

You must configure the HTTP port on the Recording Server and open this port on the firewall.

Step 13 Select **OK** or **Apply**.

Configuring an Alternate Cisco Unified Videoconferencing Desktop Server to Manage Recording

If you select an alternate server to manage recording, you can configure neither recording settings nor manage recordings.

Before You Begin

- Navigate to the Cisco Unified Videoconferencing Desktop Server Administration web user interface.

Procedure

Step 1 Select **Recording** in the sidebar.

Step 2 Select the **Settings** tab.

Step 3 Select the **Allow playback of recordings from an alternate** Desktop **server** check box.

Step 4 Enter the URL of the alternate Desktop Server in the **Server URL** field.

Step 5 Select **OK** or **Apply**.

Calculating Space Needed for Recording

Use the following formula to calculate the space required for recordings:

recording bandwidth (in Mbytes) × time (in seconds) + 20% overhead

For example, for a call of 1 hour at 384 Kbps, calculate as follows:

384 Kbps × (60 minutes × 60 seconds) = 1382400 Kbits

1382400 ÷ 1024 = 1350 Mbits

1350 ÷ 8 = 168.75 Mbytes

168.75 × 20% = 33.75 (overhead)

168.75 + 33.75 = 202.5 Mbytes (including overhead)

Configuring Cisco Unified Videoconferencing Manager for Recording

You can use Cisco Unified Videoconferencing Manager to automatically record either a virtual room or a scheduled meeting when the meeting begins. In this case Desktop records the meeting unless one of the following problems interferes with recording:

- There are not enough available recording ports on the Desktop at the time when the meeting is scheduled
- There is not enough disk space the disk on which recordings are stored
- The maximum number of simultaneous recordings is reached

If the deployment in use comprises multiple Cisco Unified Videoconferencing Desktop Servers, automatic recording is performed on all Cisco Unified Videoconferencing Desktop Servers and several identical recordings are created. In this case it is advisable to allow one of the Cisco Unified Videoconferencing Desktop Servers to perform automatic recording, while disabling the automatic recording feature on the rest of the Cisco Unified Videoconferencing Desktop Servers in the deployment.

- Allowing Recording by Specified Roles, page 3-20
- Allowing Recording by Specified Users, page 3-20
- Enabling Recording for Specified Virtual Rooms, page 3-20

Allowing Recording by Specified Roles

Procedure

Step 1 Select **Advanced Settings** in the sidebar menu.

Step 2 Select **Default User Settings**.

Step 3 Select an option from the **Recording Policy** field.

Or

Step 4 Select **Allow everyone to record** to enable recording permission for endpoint-initiated ad hoc conferences that do not belong to a specific user.

Step 5 Select **OK** to save your changes.

Allowing Recording by Specified Users

Procedure

Step 1 Select **User Management** in the sidebar menu.

Step 2 Select **Users**.

Step 3 Select the link in the **Name** column for the user you require.

Step 4 Select **Advanced**.

Step 5 (Optional) Select **Inherit recording policy from Default User Settings** to define custom recording policy for this user.

Step 6 Select **OK** to save your changes.

Enabling Recording for Specified Virtual Rooms

Procedure

Step 1 Select **User Management** in the sidebar menu.

Step 2 Select **Users**.

Step 3 Select the link in the Name column for the user you require.

Step 4 Select **Virtual Room Setting**.

Step 5 To automatically record a meeting when the meeting starts, select **Record the meeting when meeting starts**. This option is available if

- Recording is allowed for the current user according to the recording policy.
- The **Record Meeting** field is set to **Enabled under Admin > Advanced Settings > Look and Feel**.

  The meeting is not recorded if there are not enough available recording ports on the Desktop when the meeting is scheduled.

Step 6 Select **OK** to save your changes.

Configuring a Gatekeeper

This section describes how to set a gatekeeper to work in Call Setup (Q.931) and Call Control (H.245) Routed Mode to enable Cisco Unified Videoconferencing Solution deployments without Cisco Unified Videoconferencing Manager to operate correctly.

Note Do not configure a gatekeeper if using a deployment with Cisco Unified Videoconferencing Manager. For more information about gatekeeper design options, see the Cisco Unified Videoconferencing Solution Reference Network Design (SRND) at http://www.cisco.com/en/US/products/ps10463/products_implementation_design_guides_list.html.

Procedure

Step 1 Select Cisco IOS H.323 Gatekeeper in the sidebar of the Administrator interface.

Step 2 Select **Settings**.

Step 3 Select **Calls**.

Step 4 In the Routing mode field, select **Call Setup (Q.931) and Call Control (H.245)**.

Step 5 Select **Upload** to save the change.

How to Configure Cisco Unified Videoconferencing Desktop Server to Allow Streaming

- Desktop Server Limitations, page 3-22
- Configuring This Desktop Streaming Server to Manage Streaming, page 3-22
- Configuring Streaming for Playback Using the UDP Connection, page 3-24
- How to Enable Streaming Over Port 80, page 3-24

Desktop Server Limitations

These are limitations of Cisco Unified Videoconferencing Desktop Server streaming:

- To establish synchronized moderated streaming, select a single streaming server to be used by all Cisco Unified Videoconferencing Desktop Servers.
- On each Cisco Unified Videoconferencing Desktop Server, define an alternate streaming server and URL to enable a moderator on any Cisco Unified Videoconferencing Desktop Server to allow streaming across all the Cisco Unified Videoconferencing Desktop Servers.
- An independent Cisco Unified Videoconferencing Desktop Server with its own streaming server can be enabled only by a moderator on that server.
- By default, streaming works with TCP buffering on the Internet. However, you can configure streaming to use UDP. In cases where you need to use UDP for internal connections while using TPC for external connections, configure Cisco Unified Videoconferencing Solution for UDP with TCP fallback and block the UDP traffic for external users.
- UDP transport provides lower latency on a local network with no packet loss.

Guidelines for Configuring Streaming in Load Balancing Deployments

- In load balancing deployments, you must install Streaming Server on all servers deployed.
- Use external addresses for the Streaming Server address and the Desktop network interface.
- Enable streaming for all Cisco Unified Videoconferencing Desktop Servers in the deployment.

Configuring This Desktop Streaming Server to Manage Streaming

By default, the Cisco Unified Videoconferencing Desktop Server is configured to allow streaming over the TCP port 7070. If necessary, you can configure a different port for streaming.

During this procedure you configure the following:

- IP address of the Cisco Unified Videoconferencing Streaming Server—The address is used for communications with the Cisco Unified Videoconferencing Desktop Server, as well as for external access if the public address is not defined.
- Public address—The address that clients use to access the Cisco Unified Videoconferencing Streaming Server. You can use either a unique IP address or a DNS address if there is an internal and an external IP address.
- TCP port number—By default, this is port 7070. This port must be open on the firewall.

If streaming is disabled for this Cisco Unified Videoconferencing Desktop Server, you can enable users to watch webcasts from the Desktop portal using an alternate Cisco Unified Videoconferencing Desktop Server. In this case you need to provide the alternate Cisco Unified Videoconferencing Desktop Server URL.

Before You Begin

- Navigate to the Desktop Server Administration web user interface.
- Select **Deployment** in the sidebar and verify that streaming is enabled on the Servers page.

Procedure

Step 1 Select **Streaming** in the sidebar of the Cisco Unified Videoconferencing Desktop Server Administration user interface.

The **Settings** tab is displayed.

Step 2 Choose a bit rate value to define the Standard Definition and High Definition streaming feed rates between the MCU and the Desktop Server. Set the Standard Def and High Def rates.

Step 3 Also as in the recording section we will jump down to the standard def rate if the MCU can not support a HD connection.

Step 4 Enter the IP address of the streaming server.

Note The indicator next to the **Streaming Server Address** field indicates whether or not the connection to the target server is successful.

Step 5 If necessary, configure multicast settings:

a. Check the **Enable Multicast** option.

Enter the multicast IP address.

The valid multicast IP address is in the range of 224.0.0.1 and 239.255.255.255.

b. Enter the **Time to Live** value.

c. Define clients that will be able to watch multicasts by entering IP range in the fields and selecting the Arrow button.

Step 6 (Optional) Enter a public address. We recommend to use a public address that clients can resolve.

Step 7 Enter a TCP streaming port.

We recommend using the default port 7070.

Note If you use a TCP port different from the default value of 7070, you must open this port on the firewall. For more information about configuring a UDP connection, refer to the Configuring Streaming for Playback Using the UDP Connection, page 3-24.

Step 8 Select **OK** or **Apply**.

Configuring an Alternate Desktop Server for Watching Webcasts

For basic and advanced deployments where streaming is disabled, you can configure the Desktop Server to refer to an alternate Desktop Server which is used for streaming in order to watch webcasts.

Before You Begin

- Navigate to the Desktop Server Administration web user interface.
- Select **Deployment** in the sidebar and verify that streaming is disabled on the Servers page.

Procedure

Step 1 Select **Streaming** in the sidebar.

Step 2 Select the **Settings** tab.

Step 3 Select the **Allow watching of webcasts from an alternate** Desktop **server** check box.

Step 4 In the Server URL field, enter the URL of the alternate Desktop Server.

Step 5 Select **OK** or **Apply**.

Configuring Streaming for Playback Using the UDP Connection

This procedure describes how to allow UDP connections to streaming, in case you want to allow UDP streaming first be attempted before the default TCP on default port 7070.

Procedure

Step 1 Perform these steps on the Cisco Unified Videoconferencing Desktop Server:

a. Navigate to the following directory: *C:\Program Files\Darwin Streaming Server.*

b. Open the streamingserver.xml file.

c. Change the force_tcp parameter value to "false".

d. Save the file.

e. Restart the Cisco Unified Videoconferencing Streaming Server.

f. Restart the "Cisco Unified Videoconferencing Streaming Server" service.

Step 2 Perform these steps on the Desktop Client computer:

a. Navigate to the following directory: *%AppData%\Apple Computer\QuickTime*.

b. Delete the file QuickTime.qtp.

How to Enable Streaming Over Port 80

Enabling streaming over port 80 is performed in the following steps:

1. Binding a Cisco Unified Videoconferencing Streaming Server, page 3-25
2. Enabling Streaming Over Port 80, page 3-25
3. Binding an Apache Tomcat to a Specific IP Address, page 3-27

Binding a Cisco Unified Videoconferencing Streaming Server

If the Cisco Unified Videoconferencing Streaming Server runs on the same server as Cisco Unified Videoconferencing Desktop Server, you need to bind it to a separate NIC or IP address on the PC so that it does not conflict with port 80 access to the Cisco Unified Videoconferencing Desktop Server portal. Alternatively, you can deploy the Cisco Unified Videoconferencing Streaming Server on a separate server.

This procedure describes how to configure the Cisco Unified Videoconferencing Streaming Server to bind it to a specific IP.

Procedure

Step 1 Open the *streamingserver.xml* file at

C:\Program Files\Darwin Streaming Server.

Step 2 Find the property **bind_ip_addr**:

```
<PREF NAME="bind_ip_addr">0</PREF>
```

By default, this property is set to a value of zero which indicates that all IP addresses are enabled for the server.

Step 3 Replace the zero with the IP address to which you wish to bind (for example, 1.2.3.4):

```
<PREF NAME="bind_ip_addr">1.2.3.4</PREF>
```

Step 4 Save the *streamingserver.xml* file as a plain text file (not as .rtf or any other format).

Enabling Streaming Over Port 80

Procedure

Step 1 Find the section for the **rtsp_port** property in the same *streamingserver.xml* file.

Step 2 By default, the following values are present:

```
<LIST-PREF NAME="rtsp_port" TYPE="UInt16">
    <VALUE>7070</VALUE>
    <VALUE>554</VALUE>
    <VALUE>8000</VALUE>
    <VALUE>8001</VALUE>
</LIST-PREF>
```

Step 3 Add the following entry:

```
<VALUE>80</VALUE>
```

To force streaming only over port 80, you can remove some of the other values but you must leave the value for port 554, as this is the port over which the Cisco Unified Videoconferencing Streaming Server monitors administrative functions as well as RTSP.

The code should look as follows:

```
<LIST-PREF NAME="rtsp_port" TYPE="UInt16">
    VALUE>80</VALUE>
    <VALUE>554</VALUE>
</LIST-PREF>
```

Step 4 Save the *streamingserver.xml* file as a plain text file (not as .rtf or any other format).

Step 5 Restart the Cisco Unified Videoconferencing Streaming Server.

Binding an Apache Tomcat to a Specific IP Address

Procedure

Step 1 Open the *server.xml* file at

C:\Program Files\Cisco\Cisco Unified Videoconferencing Desktop\tomcat\conf.

Step 2 Add the *address="1.2.3.4"* field in the port 80 connector definition as follows, and restart Tomcat:

```
<!-- Define a non-SSL HTTP/1.1 Connector on port 8080 -->
<Connector port="80" maxHttpHeaderSize="8192"
    maxThreads="130"
    minSpareThreads="25"
    maxSpareThreads="75"
    enableLookups="false"
    redirectPort="8443"
    acceptCount="300"
    connectionTimeout="20000"
    disableUploadTimeout="true"
    address="1.2.3.4" />
```

where 1.2.3.4 is the IP address you want to bind to.

Step 3 Select **Streaming** in the Cisco Unified Videoconferencing Desktop Server Administration user interface.

Step 4 Enter the Tomcat IP address in the **Streaming Server Address** field.

Step 5 Enter the IP address or DNS name in the **Streaming Server Virtual Address** field but do not specify a specific port.

Note Users connecting from behind an HTTP Proxy may need to modify their client-side Quicktime Player transport settings to default to HTTP tunneling.

Step 6 Save the *server.xml* file as a plain text file (not as .rtf or any other format).

How to Configure Third-Party Equipment

This section describes how to configure third-party communication and security equipment used in Cisco Unified Videoconferencing Solution deployments.

- Configuring a Firewall, page 3-27

Configuring a Firewall

Verify that the firewall is properly configured according to a topology described in Chapter 2, "Selecting a Deployment Topology".

- Firewall Guidelines, page 3-28
- Ports to Open in the Firewall to Allow Streaming, page 3-28

Firewall Guidelines

- Firewall Configuration Guidelines, page 3-28
- NAT Configuration Guidelines, page 3-28

Firewall Configuration Guidelines

This section describes the simplest and most typical firewall configuration. A typical configuration allows any computer located on an private network to reach a DMZ and external networks. A computer on an external network can access some specific services in the DMZ but not the private network. In contrast to this, a host located in the DMZ can access the external networks as well as some specific services on specific servers, but not the entire private network.

The firewall system uses the following interfaces to control different network types:

- WAN—Controls access to and from unprotected external networks, for example a public internet or a partner organization network.
- DMZ—Controls a DMZ network protected by the firewall.
- LAN—Controls a private network protected by the firewall.

Related Topics

- Firewall Rules, page D-1

NAT Configuration Guidelines

Network address translation (NAT) is supported for the following traffic directions:

- From DMZ to external networks
- From internal networks to external networks

Traffic is not allowed between internal networks and the DMZ because NAT configuration between internal networks and the DMZ is not supported by Cisco Unified Videoconferencing Solution Release 7.1.

A firewall rule must be added for each NAT table entry described in this section to permit traffic through the NAT rule. For deployments that do not implement NAT, add a firewall rule corresponding to the following NAT table entries to permit the associated traffic.

Note On most firewalls it is not possible to access NAT services using the WAN IP address from within internal networks or a DMZ network.

Related Topics

- NAT Rules, page D-5

Ports to Open in the Firewall to Allow Streaming

To configure the firewall to allow streaming, you must open a number of ports including:

- Ports from the user to the Cisco Unified Videoconferencing Streaming Server
- TCP port 7070 (or other port of choice) for tunneled RTSP
- Ports for Cisco Unified Videoconferencing Desktop Server to the Cisco Unified Videoconferencing Streaming Server
- UDP ports 6972-65535
- TCP port 554

Sometimes firewalls are configured to block packets used for streaming media. Two general options exist for crossing the firewall boundary: either configure the firewall to allow streaming packets, or reconfigure the streaming server and client to use different network protocols that cross the firewall boundary.

The Streaming Server uses the IETF RTSP/RTP protocols. RTSP runs on top of TCP, while RTP runs over UDP. Many firewalls are configured to restrict TCP packets by port number and are very restrictive on the UDP. The streaming server can tunnel RTSP/RTP traffic through HTTP (the protocol used by web servers and web browsers).

Some firewalls may inspect traffic on port 80 and not allow the tunneled RTSP/RTP on that port. For this reason, we recommend that you use an alternate TCP port for HTTP tunneling such as the QuickTime de facto standard port 7070. This is configured in the streaming server by default as long as you specify the port as part of the streaming server virtual address in the **Streaming** section of the Cisco Unified Videoconferencing Desktop Server Administration user interface.

CHAPTER 4

Configuring Cisco Unified Videoconferencing Desktop Servers for Scalability and High Availability

- Scalability with Round Robin DNS, page 4-1
- Scalability with Generic Load Balancer, page 4-2
- Scalability with Radware WSD, page 4-7

Scalability with Round Robin DNS

Cisco Unified Videoconferencing Desktop Servers can be configured for scalability and high availability by placing several of them in a Tomcat cluster and using a Round Robin DNS on the DNS server to route requests to the different servers within the cluster.

- Round Robin DNS Functionality, page 4-1
- Round Robin DNS Limitations, page 4-2

Round Robin DNS Functionality

In a deployment with Round Robin DNS, a single DNS name resolves to multiple IP addresses defined by the network administrator. Each request is resolved to one of the Cisco Unified Videoconferencing Desktop Servers in the cluster. The list of addresses for external clients are typically different from those within the company network. The DNS name is resolved to one of the defined IP addresses for each client request.

Servers in the cluster are recommended to have two network cards, one to connect to an isolated network behind the load balancer and a second card to connect to the company network.

The integrity of authenticated HTTP sessions is maintained when requests are routed to different servers, enabling rerouting to different Cisco Unified Videoconferencing Desktop Servers within the cluster without requiring another login.

Round Robin DNS Limitations

Users in the same meeting could be routed to different Cisco Unified Videoconferencing Desktop Servers. This can be costly, as each Cisco Unified Videoconferencing Desktop Server occupies an extra port, thereby increasing the number of servers per meeting, reducing the efficiency of port usage.

Spreading meeting participants over more than one server also implies that participants on other servers lose chat and raising hand functionality.

There is no guarantee that the load is distributed evenly when using Round Robin DNS.

Scalability with Generic Load Balancer

Cisco Unified Videoconferencing Desktop Servers in a Tomcat cluster can also be managed using a generic load balancer. This topology has the added advantage of continued service even when one or more of the servers have failed.

- Generic Load Balancer Functionality, page 4-2
- How to Configure Round Robin DNS and Generic Load Balancers, page 4-2
- Generic Load Balancer Limitations, page 4-7

Generic Load Balancer Functionality

Generic load balancers offer the continued service of a cluster when one or more of the units are unresponsive, due to the health checks that take place in the background. If one or more of the servers are not able to respond, the load balancer reroutes requests to the remaining active servers.

We recommend using the health checks of ICMP echo request and HTTP Web (TCP port 80) to monitor the server farm in your deployment.

External clients access the IP address of the cluster, like cluster.x.com, which points to the load balancer via the firewall. The load balancer in turn resolves the request to one of the servers in the cluster. The firewall must be configured with a static IP mapping. Internal clients type the same address, cluster.x.com, which internally resolves directly to the load balancer.

Note The scalability cannot be extended to streaming servers.

How to Configure Round Robin DNS and Generic Load Balancers

A Tomcat cluster enables users to access the Cisco Unified Videoconferencing Desktop Servers using a single DNS name, for example sdcluster.x.com, routing to three servers each with their own IP address.

- Configuring DNS Settings for Round Robin DNS, page 4-3
- Configuring DNS Settings for Generic Load Balancers, page 4-3
- Configuring the Tomcat Cluster, page 4-3
- Configuring Cisco Unified Videoconferencing Desktop in a Cluster, page 4-4
- Configuring Multiple NIC Servers, page 4-5

- Configuring Streaming and Recording for Scalability, page 4-6
- Configuring Load Balancer Routing Rules, page 4-6

Configuring DNS Settings for Round Robin DNS

Procedure

Step 1 Define a single DNS name for the multiple IP addresses in the cluster.

Step 2 Define a DNS name for each of the servers in the cluster, each associated with that server's IP address.

Note This DNS name must be available from all locations that might request access to the Cisco Unified Videoconferencing Desktop Servers.

Configuring DNS Settings for Generic Load Balancers

Procedure

Step 1 Define a single DNS name for the a single IP address that represents the cluster.

Step 2 Define a DNS name for each of the servers in the cluster, each associated with that server's IP address.

Note This DNS name must be available from all locations that might request access to the Cisco Unified Videoconferencing Desktop Servers.

Configuring the Tomcat Cluster

This procedure configures the Tomcat cluster as a simple TCP cluster with full memory replication of sessions. On each of the servers in the cluster, perform the following steps.

Procedure

Step 1 Open the file server.xml on each Cisco Unified Videoconferencing Desktop Server located at *c:\Program Files\Cisco\cuvcd\tomcat\conf*.

Step 2 Locate the line

```
<Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"
channelSendOptions="8">
```

Step 3 Replace that line with the following code:

```
<Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"
channelSendOptions="8"><Manager
```

```
className="org.apache.catalina.ha.session.DeltaManager"expireSessionsOnS
hutdown="false"notifyListenersOnReplication="true"/><Channel
className="org.apache.catalina.tribes.group.GroupChannel"><Membership
className="org.apache.catalina.tribes.membership.McastService"address="2
28.0.0.4"port="45564"frequency="500"dropTime="3000"/><Receiver
className="org.apache.catalina.tribes.transport.nio.NioReceiver"address=
"auto"port="4000"autoBind="100"selectorTimeout="5000"maxThreads="6"/>
<Sender
className="org.apache.catalina.tribes.transport.ReplicationTransmitter">
<Transport
className="org.apache.catalina.tribes.transport.nio.PooledParallelSender
"/></Sender><Interceptor
className="org.apache.catalina.tribes.group.interceptors.TcpFailureDetec
tor"/><Interceptor
className="org.apache.catalina.tribes.group.interceptors.MessageDispatch
15Interceptor"/></Channel><Valve
className="org.apache.catalina.ha.tcp.ReplicationValve"filter=""/><Valve
className="org.apache.catalina.ha.session.JvmRouteBinderValve"/>
<Deployer
className="org.apache.catalina.ha.deploy.FarmWarDeployer"tempDir="/tmp/w
ar-temp/"deployDir="/tmp/war-deploy/"watchDir="/tmp/war-listen/"watchEna
bled="false"/><ClusterListener
className="org.apache.catalina.ha.session.JvmRouteSessionIDBinderListene
r"/><ClusterListener
className="org.apache.catalina.ha.session.ClusterSessionListener"/>
</Cluster>
```

Step 4 Open the file *web.xml* in *\tomcat\webapps\cuvm\WEB-INF*.

Step 5 Add a line and enter `<distributable/>`.

Step 6 Save and close the file.

Step 7 Open the file *context.xml* in *\tomcat\conf*.

Step 8 Locate the line containing `<Manager pathname="" />`.

Step 9 Delete this line.

Step 10 Save and close the file.

Step 11 Restart the server.

Configuring Cisco Unified Videoconferencing Desktop in a Cluster

Procedure

Step 1 Enter the same DNS name for each of the servers in the cluster during installation.

a. Run the installation of the Cisco Unified Videoconferencing Desktop Server.

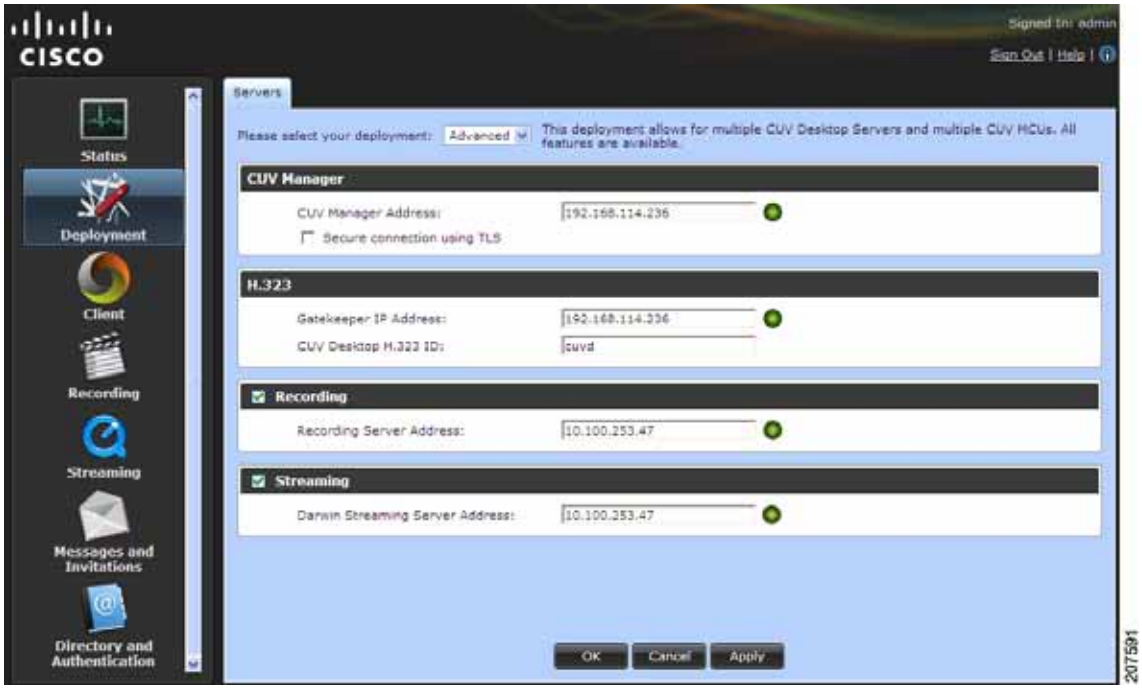
b. Enter the DNS name in the Desktop **Fully Qualified Domain Name** field in the Desktop Hostname Configuration window.

Step 2 Define the same IP address in the **Cisco Unified Videoconferencing Manager Address** field for each of the servers in the cluster.

a. Open the Cisco Unified Videoconferencing Desktop Server Administration Web User Interface.

b. Select the **Deployment** section (Figure 4-1 on page 4-5).

Figure 4-1 Setting IP Addresses of Associated Servers



c. Enter the IP address in the **Cisco Unified Videoconferencing Manager Address** field, identical to the other servers in the cluster.

d. Ensure the Recording and Streaming sections are disabled.

e. Repeat for each of the servers in the cluster.

Step 3 Repeat Step 2 for the **Gatekeeper IP Address** field.

Configuring Multiple NIC Servers

Procedure

Step 1 Open server.xml on each Cisco Unified Videoconferencing Desktop Server located at *c:\Program Files\Cisco\cuvcd\tomcat\conf.*

Step 2 Locate the line

```
<Membership
className="org.apache.catalina.tribes.membership.McastService"
```

Step 3 Use the bind attribute to define the IP interface to restrict cluster membership multicast messages. For example:

```
<Membership
className="org.apache.catalina.tribes.membership.McastService"address="2
28.0.0.4"port="45564"frequency="500"dropTime="3000"bind="10.0.0.2"/>
```

Configuring Streaming and Recording for Scalability

Currently there is no solution for recording when the Cisco Unified Videoconferencing Desktop Server is configured for scalability. Therefore recording functionality must be disabled on each Cisco Unified Videoconferencing Desktop Server used for interactive users (Figure 4-1 on page 4-5).

To support streaming functionality in the cluster, you can install dedicated Cisco Unified Videoconferencing Desktop Servers as streaming servers, and enable streaming as a policy on all scheduled meetings and Virtual rooms. The maximum number of streaming servers is the number of Cisco Unified Videoconferencing Desktop Servers deployed for interactive users.

To configure a dedicated streaming server, you can either point all interactive Cisco Unified Videoconferencing Desktop Servers to the same alternate streaming server, or assign one streaming server to each interactive Cisco Unified Videoconferencing Desktop Server as the alternate streaming server.

Procedure

Step 1 Open the Cisco Unified Videoconferencing Desktop Server Administration Web User Interface.

Step 2 Select the **Deployment** section (Figure 4-1 on page 4-5).

Step 3 Select the **Streaming** check box.

Step 4 Select the check box **Allow watching of webcasts from an alternate** Cisco Unified Videoconferencing Desktop Server

Step 5 Enter the IP address of the dedicated streaming server.

Step 6 Configure the Cisco Unified Videoconferencing Manager to enable streaming for virtual rooms and scheduled meetings (see the *User Guide for Cisco Unified Videoconferencing Manager* for further details).

Configuring Load Balancer Routing Rules

Procedure

Step 1 Set the persistence based on JSESSIONID in HTTP header, otherwise on source IP.

Step 2 Select sever based on least amount of traffic or fastest response time. This will insure that all severs are as evenly loaded as possible.

Generic Load Balancer Limitations

Users in the same meeting could be routed to different Cisco Unified Videoconferencing Desktop Servers. This can be costly, as each Cisco Unified Videoconferencing Desktop Server occupies an extra port, thereby increasing the number of servers per meeting, reducing the efficiency of port usage.

Spreading meeting participants over more than one server also implies that participants on other servers lose chat and raising hand functionality.

Scalability with Radware WSD

Cisco Unified Videoconferencing Desktop Servers can also be made scalable using Radware WSD. This configuration does not use Tomcat clustering. Configure each Cisco Unified Videoconferencing Desktop Server independently.

- Radware WSD Functionality, page 4-7
- How to Configure Radware WSD, page 4-7
- Radware WSD Limitations, page 4-11

Radware WSD Functionality

Radware WSD's application, the App Director, can be configured to track the meeting ID, enabling it to route users in the same meeting to a single Cisco Unified Videoconferencing Desktop Server. The WSD routes one meeting to one server, and when one is full, it reroutes other meetings to one of the remaining servers.

When a request arrives to the main virtual IP address, the App Director inspects the cookie embedded within the URL to determine if this request is part of an existing session with its server location. If it is, the App Director redirects the HTTP request to that server.

When a new session is requested, the App Director can be configured to route requests to the server with the least amount of traffic.

The WSD does not require the use of an extra port for each meeting, since there is always only one server per meeting.

How to Configure Radware WSD

- Configuring Network Interfaces in WSD, page 4-8
- Configuring Routing in WSD, page 4-8
- Configuring the Central Server Farm, page 4-8
- Configuring Remaining Servers in the Farm, page 4-9
- Configuring Layer 4 Policies, page 4-9
- Configuring Servers of the Central Server Farm, page 4-10
- Configuring a Single Server Farm Server, page 4-10
- Configuring Cookie Persistency, page 4-11

Configuring Network Interfaces in WSD

Procedure

Step 1 Open the App Director.

Step 2 Select **Router**.

Step 3 Select **IP Router**.

Step 4 Select **Interface Parameters**.

Step 5 Configure the IP interfaces for the device. One interface is the IP address to access the load balancer from outside and inside the network. The other interface is the load balancer's IP address on the isolated network of the Cisco Unified Videoconferencing Desktop Server farm.

Configuring Routing in WSD

Procedure

Step 1 Open the App Director.

Step 2 Select **Router**.

Step 3 Select **Routing Table**.

Step 4 Configure the routing table so that traffic that is destined for the Cisco Unified Videoconferencing Desktop Servers is routed through one interface, while all other traffic is routed through the other interface.

Note Routes can only be defined when the interface is accessible.

Configuring the Central Server Farm

Procedure

Step 1 Open the App Director.

Step 2 Select **Farms**.

Step 3 Select **Farm Table**.

Step 4 Select **Create**.

Step 5 Enter the central server farm name in the **Farm Name** field, for example Central_Server_Farm.

Step 6 Enter 90000 in the **Aging Time** field.

Step 7 Select **Least Amount of Traffic** in the **Dispatch Method** field.

Step 8 Select **Server Per Session** in the **Session Mode** field.

Step 9 Select **TCP Port** in the **Connectivity Check Method** field.

Step 10 Select **HTTP Redirection** in the **Redirection Mode** field.

Step 11 Select **IP Mode** in the **HTTP Redirection Mode** field.

Step 12 Use the default values for the remaining fields.

Step 13 Select **Set**.

Configuring Remaining Servers in the Farm

Perform the following procedure on each of the remaining servers in the farm:

Procedure

Step 1 Open the App Director.

Step 2 Select **Farms**.

Step 3 Select **Farm Table**.

Step 4 Select **Create**.

Step 5 Enter the name of this server in the farm in the **Farm Name** field.

Step 6 Enter 60 in the **Aging Time** field.

Step 7 Select **Least Amount of Traffic** in the **Dispatch Method** field.

Step 8 Select **Server Per Session** in the **Session Mode** field.

Step 9 Select **TCP Port** in the **Connectivity Check Method** field.

Step 10 Use the default values for the remaining fields.

Step 11 Select **Set**.

Configuring Layer 4 Policies

Procedure

Step 1 Open the App Director.

Step 2 Select **Servers**.

Step 3 Select **Layer 4 Farm Selection**.

Step 4 Select **Layer 4 Policy Table**.

Step 5 Select **Create**.

Step 6 Enter the IP address of the central server farm in the **Virtual IP** field.

Step 7 Select **Any** in the **L4 Protocol** field.

Step 8 Enter a policy name in the **L4 Policy** Name field. For example, Main_Policy.

Step 9 Enter the name of the central server farm in the **Farm Name** field. For example, Central_Server_Farm.

Step 10 Use the default values for the remaining fields.

Step 11 Select **Set**.

Configuring Servers of the Central Server Farm

Procedure

Step 1 Open the App Director.

Step 2 Select **File** > **Configuration** > **Receive From Device**.

Step 3 Select ASCII as the file format.

Step 4 Select **Set**.

Step 5 Search for the name of each farm and note its IP address.

For example, `rsWSDFarmName.0.0.0.2="S1_Farm"` denotes S1_Farm's IP address is 0.0.0.2

Step 6 Open the App Director.

Step 7 Select **Servers**.

Step 8 Select **Application Servers**.

Step 9 Select **Table**.

Step 10 Select **Create**.

Step 11 Enter the name of the central server farm in the **Farm Name** field. For example, Central_Server_Farm.

Step 12 Enter the IP address of the server in the farm in the **Server Address** field (see Step 5).

Step 13 Enter a name for this server in the **Server Name** field. For example, S1-Redir_To_S1_Farm.

Step 14 Select **Local Farm** in the **Type** field.

Step 15 Enter the IP address of the server's L4 policy in the **Redirect To** field.

Step 16 Use the default values for the remaining fields.

Step 17 Select **Set**.

Configuring a Single Server Farm Server

Procedure

Step 1 Open the App Director.

Step 2 Select **Servers**.

Step 3 Select **Application Servers**.

Step 4 Select **Table**.

Step 5 Select **Create**.

Step 6 Enter the name of the single server farm in the **Farm Name** field. For example, S1_Farm.

Step 7 Enter the IP address of the server in the **Server Address** field.

Step 8 Enter the name of the server in the **Server Name** field. For example, S1.

Step 9 Use the default values for the remaining fields.

Step 10 Select **Set**.

Note You may configure an additional server as a backup server for a farm in case of server failure. On the backup server, select **Backup** in the **Operation Mode** field.

Configuring Cookie Persistency

Procedure

Step 1 Open the App Director.

Step 2 Select **Layer 7 Server Persistency**.

Step 3 Select **Text Match**.

Step 4 Select **Create**.

Step 5 Enter the name of the farm in the **Farm Name** field. For example, Central_Server_Farm.

Step 6 Select **URL Cookie** in the **Lookup Mode** field.

Step 7 Enter CONFID in the **Persistency Identifier** field.

Step 8 Enter & in the **Stop Chars** field.

Step 9 Enter 90000 in the Select **Enabled** in the **Ignore Source IP** field.**Inactivity Timeout [sec]** field.

Step 10 Select **Enabled** in the **Ignore Source IP** field.

Step 11 Use the default values for the remaining fields.

Step 12 Select **Set**.

Radware WSD Limitations

A redirected request does not maintain session authentication, since reroutes use specific IP addresses. This requires users to re-enter credentials when their requests are rerouted.

CHAPTER 5

Testing your Cisco Unified Videoconferencing Solution Deployment

- Testing Desktop Connectivity, page 5-1
- Testing Room System Connectivity and Moderation, page 5-2
- Testing Webcast Access, page 5-2
- Testing gateway Functionality, page 5-3
- Testing Load Balancing, page 5-3
- Finding Further Information, page 5-4

Testing Desktop Connectivity

Procedure

Step 1 Verify that your video and audio peripheral equipment is connected to your desktop PC and configured correctly.

Step 2 From a client machine (with Windows XP Service Pack 2 or higher), connect to Cisco Unified Videoconferencing Desktop Server via the following URL:

http://<FQDN>/cuvm

Step 3 You are prompted to install Desktop Client.

Note If you have not yet installed Desktop Client or if you need to update your version of Desktop Client, a yellow message displays on Cisco Unified Videoconferencing Desktop Server entry page. Select the link to access the page from which you can install Desktop Client.

Step 4 After installing Desktop Client, enter a meeting ID in Cisco Unified Videoconferencing Desktop Server that starts with one of the following:

- The prefix configured on your Cisco Unified Videoconferencing 3500 MCU for the Desktop service.
- A valid Cisco Unified Videoconferencing Manager virtual room ID.

The Desktop Client loads and your own video stream is displayed.

Note Ensure there is no firewall enabled on your machine that might block the Desktop Client.

Testing Room System Connectivity and Moderation

This procedure describes how to test room system connectivity and moderation inside an enterprise private network. This procedure describes how to check whether or not the room system is connected to Cisco Unified Videoconferencing Desktop Server.

Procedure

Step 1 Check whether or not you are connected to the Cisco Unified Videoconferencing Desktop Server.

Step 2 Select **Moderate** in the Desktop Live Meeting Console, and then **Invite**.

Step 3 Enter the E.164 address of the room system, or its IP address if it is not registered to the Cisco IOS H.323 Gatekeeper.

The room system joins the meeting, validating room system connectivity as well as moderation.

Note To test an HD room system connectivity, use the HD service.

Testing Webcast Access

Procedure

Step 1 Check whether or not you are connected to the Cisco Unified Videoconferencing Desktop Server.

Step 2 Select **Moderate** in the Desktop Live Meeting Console, and then **Enable Streaming**.

Step 3 From another client machine (Windows XP Service Pack 2 or MAC Intel based), connect to Cisco Unified Videoconferencing Desktop Server via the following URL:

http://<FQDN>/cuvm

Step 4 Select the **Watch Webcast** link.

Step 5 Enter the meeting ID that you used in Step 2.

The Desktop Client window loads and your own video stream is displayed.

Step 6 Select **Watch**.

Step 7 Install the plug-in required to see the webcast.

Step 8 Restart your web browser to view the webcast.

Testing Gateway Functionality

This procedure describes how to test connectivity and moderation for room systems located on the ISDN/PSTN network. This procedure also describes how to check whether or not the room system is connected to the Cisco Unified Videoconferencing Desktop Server via a gateway.

Procedure

Step 1 Check your connection to the Cisco Unified Videoconferencing Desktop Server.

Step 2 Select **Moderate** in the Desktop Client window, and then **Invite**.

Step 3 Enter the gateway service ID followed by the room system number as it appears on the ISDN/PSTN network.

The room system joins the meeting, validating room system connectivity via gateway as well as moderation.

Note To test an HD room system connectivity, use the HD service.

Testing Load Balancing

Perform this test only for load balancing deployments:

Procedure

Step 1 Establish a conference.

Step 2 Connect several Desktop Clients to this conference.

Step 3 Access the Cisco Unified Videoconferencing Desktop Server Administration web interface.

Step 4 Select **Status** in the sidebar.

Step 5 In the Live Ports area, verify the number of clients associated with this server.

Step 6 Repeat 2 - 5 for other Cisco Unified Videoconferencing Desktop Servers in the deployment.

Finding Further Information

For more information on issues such as these

- Product troubleshooting
- Cisco WebEx integration
- IBM Sametime integration
- Microsoft OCS integration
- Cisco Unified Videoconferencing Manager scheduling deployment options
- Cisco Unified Videoconferencing Manager Network Manager deployment
- Cisco Unified Videoconferencing 5000 Series MCU Quality of Service settings

Refer to the following Cisco publications:

- *Configuration Guide for Cisco Unified Videoconferencing Manager Release 7.1*
- *Troubleshooting Guide for Cisco Unified Videoconferencing Manager Release 7.1*
- *Troubleshooting Guide for Cisco Unified Videoconferencing 3500 Gateway Release 5.5 and 5.6*
- *Configuration Guide for Cisco Unified Videoconferencing 5100 Series MCU Release 7.1*
- *Configuration Guide for Cisco Unified Videoconferencing 5200 Series MCU Release 7.1*
- *Troubleshooting Guide for Cisco Unified Videoconferencing 5100 Series MCU Release 7.1*
- *Troubleshooting Guide for Cisco Unified Videoconferencing 5200 Series MCU Release 7.1*
- *Installing and Configuring the Microsoft OCS Plug-in for Cisco Unified Videoconferencing Manager Release 7.1*
- *Joining Cisco Unified Videoconferencing Manager Release 7.1 Meetings from the Microsoft OCS Client*
- *Enabling Cisco Unified Videoconferencing Manager Release 7.1 and Cisco WebEx Integration*
- *User Guide for Using the Cisco Unified Videoconferencing Desktop Connector Plug-In Release 7.1 with IBM Lotus Sametime*
- *Installing and Configuring the Cisco Unified Videoconferencing Desktop Connector Plug-In Release 7.1 with IBM Lotus Sametime*

APPENDIX A

Configuring Secure Connection Between Cisco Unified Videoconferencing Solution Components

To provide a secure access to Cisco Unified Videoconferencing Solution components and to secure connection between them, you need to configure the components to use one of these cryptographic protocols: HTTPS, TLS, or SSL. If it is required that only HTTPS be used to access web pages, use Configuring Windows Firewall, page A-12.

Procedures included in this appendix mention Cisco Unified Videoconferencing Desktop Server default installation location. If you used a customized location during Cisco Unified Videoconferencing Desktop Server installation, modify paths in procedures appropriately.

- About Server Certificates, page A-1
- Configuring Secure Access to the Cisco Unified Videoconferencing Manager, page A-2
- Configuring Secure Access to Cisco Unified Videoconferencing Desktop Server, page A-4
- Configuring Windows Firewall, page A-12
- Example of Using the Microsoft Certificate Service, page A-13

About Server Certificates

Both Cisco Unified Videoconferencing Desktop Server and Cisco Unified Videoconferencing Manager have default pre-installed certificates that are not fit for mutual authentication because they are not unique. Procedures in this section show how to use the java key tool to replace default certificates with unique server certificates. The procedures involve sending a certificate request to a Certificate Authority (CA). Depending on the security solution used in your deployment, you can either use a well known CA like Microsoft Certificate Service or in-house certificate tool. The Certificate reply needs to contain issuer information and signature sufficient to establish a certificate chain to a trusted certificate.

The java key tool comes with the version of java installed by both Desktop and Cisco Unified Videoconferencing Manager.

Configuring Secure Access to the Cisco Unified Videoconferencing Manager

The procedure in this section describes how to configure Cisco Unified Videoconferencing Manager for HTTPS access on an arbitrary port opened on the firewall. After the configuration is complete, the following URL is used to access to Cisco Unified Videoconferencing Manager: *https://<server>:<port>/cuvcmrm*.

Note If Cisco Unified Videoconferencing Manager and Cisco Unified Videoconferencing Desktop Server are installed on separate servers, the standard HTTPS port number 443 may be used. In this case the URL to access Cisco Unified Videoconferencing Manager does not require the port designation. For example, *https://<server>/cuvcmrm.*

To perform procedures described in this section you need a keytool—a java tool that is installed using either a JRE (Java Runtime Environment) or JDK (Java Development Kit). There are two methods of creating a new certificate for Cisco Unified Videoconferencing Manager are described:

- Sending a certificate request to a Certificate Authority (CA)
- Generating a self-signed certificate

Procedure

Step 1 Generate a keystore file:

a. Open a Command Prompt on the Cisco Unified Videoconferencing Manager Server.

b. Enter the command:

```
set path="<installDir>\CUVCMRM\jre\bin"
```

where <installDir> represents the actual installation path.

c. Enter the command:

```
MKDIR C:\certificate
```

d. Enter the command:

```
CD C:\certificate
```

e. Enter the following command:

```
keytool -genkey -keyalg RSA
-dname "cn=product,ou=users,ou=US,DC=Company,DC=com"
-alias product  -keypass passwd -keystore product.keystore
-storepass passwd
```

Note Do not press ENTER until the entire command is entered. Use a space before each hyphen.

Step 2 Generate a self-signed certificate:

a. Enter the following command:

```
keytool -selfcert -alias product -keypass passwd
-keystore product.keystore -storepass passwd
```

b. Continue with Step 6.

Or

Step 3 Generate the certificate-signing request:

a. Enter the command:

```
keytool -certreq -v -alias product -file product.csr -keypass passwd
-keystore icm.keystore -storepass passwd
```

b. Submit the content of the product.csr file to a CA for signing.

Step 4 After the signed certificate is returned by the CA, import this certificate into the keystore.

a. Verify that all relevant files are located in the folder you created while generating a keystore file. For example, *c:\certificate*.

b. Set the path for the keytool utility.

c. Enter the command:

```
keytool -import -alias CARoot -file <rootCertFromCA>.cer -keystore
product.keystore -storepass passwd
```

Step 5 Import the certificate response from the CA by entering the command:

```
keytool -import -trustcacerts -alias product -file
<signedCertFromCA>.cer -keystore product.keystore
-storepass passwd
```

Step 6 Install the certificate:

a. Stop the service "Cisco Unified Videoconferencing Manager".

b. Using Microsoft Notepad or Microsoft Wordpad applications, open the following file:

<installDir>\CUVCMRM\jboss\server\default\deploy\jbossweb-tomcat55.sar\server.xml,

where <installDir> represents the actual installation path.

c. Locate the section in which the connectors are defined.

d. Modify the following SSL/TLS connector parameters as described below. The necessary changes are marked in bold.

```
<!-- SSL/TLS Connector configuration using the admin devl guide
keystore -->
<Connector port="8444" address="${jboss.bind.address}"
maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
emptySessionPath="true"
scheme="https" secure="true" clientAuth="false"
keystoreFile="C://certificate/product.keystore"
keystorePass="passwd" sslProtocol = "TLS" />
<!-- -->
```

Note To disable non-SSL connections (HTTP) to Cisco Unified Videoconferencing Manager on port 8080, Microsoft Windows Firewall must be configured to block this port from external access.

e. Disable the default connector on port 8443 by placing "<!--" at the beginning of the connector definition and "-->" at the end. The necessary changes are marked in bold.

```
<!--
<Connector port="8443" address="${jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="${jboss.server.home.dir}/conf/icmservice.keystore"
keystorePass="<company>"
truststoreFile="${jboss.server.home.dir}/conf/icmservice.keystore"
truststorePass="<company>"sslProtocol = "TLS" />
-->
```

Step 7 Save the file and close Microsoft Notepad or Microsoft Wordpad.

Step 8 Start the "Cisco Unified Videoconferencing Manager" service.

Configuring Secure Access to Cisco Unified Videoconferencing Desktop Server

The procedure in this section describes how to configure secure access of Desktop Clients to Cisco Unified Videoconferencing Desktop Server. It is not possible to configure Desktop web access to accept an SSL connection on the standard 443 port because that port is already used to accept tunnelled connections from Desktop Client. This procedure explains how to configure Cisco Unified Videoconferencing Desktop Server to forward HTTPS requests to its web server.

Configuring Cisco Unified Videoconferencing Desktop Server to Use HTTPS

Procedure

Step 1 Select **Start** > **All Programs** > **Desktop** > **Config Tool**.

Step 2 Select the **Enable HTTPS** checkbox in the HTTPS tab.

Step 3 Select **Apply**.

Step 4 Update the start menu shortcut used to access the Desktop Administration web interface:

a. Select **Start** > **All Programs** > **Desktop**.

b. Right-click **Desktop - Administration** shortcut.

c. Select **Properties**.

d. Modify the value in the Target field from

C:\WINDOWS\explorer.exe https://localhost:80/cuvm/admin

to

C:\WINDOWS\explorer.exe http://your_IP/cuvm/admin

e. Select **OK**.

Step 5 Select **Add Certificate** to use an existing certificate, and follow the steps described in Configuring Conference Server with a Certificate, page A-5.

Step 6 Reboot the Cisco Unified Videoconferencing Desktop Server.

Step 7 Change URL in Invitations section of the Desktop Administration web interface:

a. Log into the Desktop Administration web interface.

b. Select **Messages and Invitations** on the sidebar.

c. Select the **Invitations** tab.

d. In the Desktop Access section, modify all URLs to use https instead of http.

Note By default, there are two URLs present in this section.

Configuring Conference Server with a Certificate

Desktop Conference Server forwards all HTTPS requests to a Tomcat Server. In order to configure Desktop with a certificate for HTTPS, import the certificate acquired from a Certificate Authority to Conference Server.

Procedure

Step 1 Stop the service "Cisco Unified Videoconferencing DesktopDesktop- Conference Server. x.x.x".

Step 2 Navigate to this location:

<CUVCDINSTALLDIR>\Confsrv

where <CUVCDINSTALLDIR> is the default installation directory.

Step 3 Run the Certificate Configuration Utility by double-clicking CertificateConfiguration.exe file.

Step 4 If the certificate is installed in the local machine's certificate store:

a. Select the **Configure Certificate via Certificate Store**.

b. Select **Select Certificate**.

c. Select the certificate from the list.

Step 5 If the certificate is in PKCS12 format:

a. Select **Configure Certificate via File Name**.

b. Browse to the PKCS12 certificate.

c. Enter the private key password for the certificate.

Step 6 Select **OK**.

Step 7 Verify that the certificate information is listed in the Selected Certificate pane.

Step 8 Select **Apply**.

Step 9 Select **OK**.

Step 10 Select **OK**.

Step 11 Start the service "Desktop- Conference Server.x.x.x".

Configuring Desktop Clients to Accept Generated Certificate Located on the Conference Server

Perform this configuration procedure to install the Cisco Unified Videoconferencing Desktop Server Certificate on a Desktop Client. If you try to connect to the server and the certificate is not installed on the client computer, the client issues a -734 error. View this error in the client call log: "#######get_verify_result error = 19, the peer certificate is invalid."

In cases of incorrect Cisco Unified Videoconferencing Desktop Server Certificate setting, the Desktop Client returns errors 21 or 26.

Procedure

Step 1 Obtain a certificate from the administrator. If you are using a known Windows CA server, a CA certificate can be obtained as follows:

a. Connect to the Certificate Authority Server at this address: *http://<serverName>/certsrv.*

b. On the Welcome Page, select Download a CA certificate, certificate chain, or CRL.

c. Select Download CA certificate chain and save it to your hard disk.

Step 2 Install the certificate on the computer using Microsoft Management Console:

a. Select **Start > Run**.

b. Type mmc and press enter.

c. From the File menu, select **Add/Remove Snap-in**.

d. Select **Add**.

e. Select Certificates, and then select **Add**.

f. Select **Computer Account** in the Certificates snap-in dialog box, and then select **Next**.

g. Select Local computer:(the computer this console is running on), and then select **Finish**.

h. Select **Close** and **OK**.

i. Verify that Microsoft Management Console shows the Certificates (Local Computer) certificate store.

j. Expand certificates by selecting **Certificates > Trusted Root Certification Authorities > Certificates**.

k. Right-click Certificates and select **All Tasks > Import**, and then select **Next**.

l. Select **Browse**, and select **Certificate**.

   By default it only shows X.509 Certificate file types, you must change this to Personal Information Exchange (*.pfx;*.p12) or All Files (*.*).), and select **Next**.

m. Select **Place all certificates in the following store**, and then verify that the Certificate store: Trusted Root Certification Authorities option is selected.

n. Select **Next**.

o. Verify the information and select **Finish**.

p. Verify that the Certificate Chain is located in the Trust Root Certification Authorities store.

Step 3 Verify that the Desktop Client can connect to the Cisco Unified Videoconferencing Desktop Server.

Configuring Secure Communication Between Cisco Unified Videoconferencing Desktop Server and Cisco Unified Videoconferencing Manager

Cisco Unified Videoconferencing Desktop Server and Cisco Unified Videoconferencing Manager communicate over the ETCP channel 3340. You may choose to secure this channel. Securing the communication channel between Cisco Unified Videoconferencing Desktop Server and Cisco Unified Videoconferencing Manager is performed in two stages:

- Configuring Cisco Unified Videoconferencing Desktop Server and Cisco Unified Videoconferencing Manager to Use Encryption, page A-7
- Enabling Mutual Authentication, page A-8

Configuring Cisco Unified Videoconferencing Desktop Server and Cisco Unified Videoconferencing Manager to Use Encryption

Besides securing communication, enabling encryption guarantees data integrity which is tested as a part of the transport level message integrity check.

Procedure

Step 1 Enable encryption on the Cisco Unified Videoconferencing Desktop Server:

a. Access the Desktop Administrator web user interface.

b. Select **Deployment** on the sidebar.

c. Select the **Secure connection using TLS** check box.

d. Select **OK**.

Step 2 Enable encryption on Cisco Unified Videoconferencing Manager:

a. Access Network Manager.

b. Select **Resource Management** on the sidebar.

c. Select the **Desktop** tab.

d. Select the required Desktop link in the table.

   The Cisco Unified Videoconferencing Desktop Server page opens.

e. Select the **Secure XML interface (SSL)** check box.

f. Select **OK**.

Enabling Mutual Authentication

After you configure Cisco Unified Videoconferencing Desktop Server and Cisco Unified Videoconferencing Manager to perform mutual authentication, they exchange their certificates during initialization of the SSL connection between them.

A certificate refers to an electronic document which incorporates a digital signature that associates a public key with an identity, in other words such information as the name of a person or an organization, their address, and so on.

SSL/TLS (Secure Sockets Layer/Transport Layer Security) connections rely on the existence of certificates. During the initialization of an SSL connection, the server must present its certificate to the client for the client to determine the server identity. The client can also present the server with its own certificate for the server to determine the client identity.

Related Topics

- About Server Certificates, page A-1

Configuring Mutual Authentication Using Self-Signed Certificates

If using self-signed certificates, instead of getting a certificate request signed by a CA, export a self-signed certificate from Cisco Unified Videoconferencing Manager and import to Cisco Unified Videoconferencing Desktop Server and vice versa.

Procedure

Step 1 To generate a self-signed certificate from the Cisco Unified Videoconferencing Manager:

a. Locate the Cisco Unified Videoconferencing Manager key store file at this location:

   <CUVCMINSTALLDIR>\cuvcmrm\jboss\server\default\conf\icmservice.keystore.

b. Copy the key store file to a temporary working folder, for example *C:\cert*.

c. Using the key tool utility, remove the default certificate from the icmservice.keystore file by entering this command:

```
keytool -delete -alias default -keystore
C:\cert\cuvcmrmicmservice.keystore -storepass cisco
```

d. Open a command line window.

e. Navigate to the JDK bin folder at this location:

   <CUVCMINSTALLDIR>\cuvcmrm\jre1.6.0_10\bin

f. Execute the following command using appropriate DN (fill in the appropriate information for your server and company):

```
keytool -genkeypair -keyalg RSA -alias cuvcrmiview -dname "cn=fully
qualified server name, OU=organization unit name, O=organization
name, L=location, ST=state, C=country" -keystore
C:\cert\cuvcmrmservice.keystore -storepass cisco -validity NNNN
-keysize 1024 -keypass cisco
```

where the validity parameter specifies period of time in days during which the certificate is valid. For example, 3650 stands for 10 years.

g. Export the certificate from the key store file, so that it can be installed for Desktop. Execute this command:

```
keytool -exportcert -alias cuvcrm -file C:\cert\cuvcrm.cer -keystore
cuvcrmservice.keystore -storepass cisco
```

The exported certificate is stored at C:\cert\cuvcmrm.cer.

h. Import the certificate reply into the keystore using the same alias that was used when generating the certificate request. Assuming the file that is returned from the certificate authority or, if using self-signed certificate, the certificate exported from Cisco Unified Videoconferencing Desktop Server or Cisco Unified Videoconferencing Manager is c:\cert\cert.crt. Execute this command:

```
keytool -import -trustcacerts -alias <alias> -file C:\cert\cert.crt
-keystore <keystore> -storepass cisco
```

Step 2 To generate a Self-Signed certificate from Desktop, do the following on the Cisco Unified Videoconferencing Desktop Server.

a. Locate the Desktop key store file at this location:

<CUVCDINSTALLDIR>\data\sds.keystore.

b. Copy the key store file to a temporary working folder, for example *C:\cert*.

c. Using the key tool utility, remove the default certificate from the sds.deystore file by entering this command:

```
keytool -delete -alias default -keystore C:\cert\sds.keystore
-storepass cisco
```

d. Open a command line window.

e. Navigate to the JDK bin folder at this location:

<CUVCDINSTALLDIR>\JRE\bin

f. Generate the private key and certificate by executing this command:

```
keytool -genkeypair -keyalg RSA -keysize 1024 -validity NNNN -dname
"cn=sds.mydomain.com, OU=organization unit name, O=organization
name, L=location, ST=state, C=country" -alias sds -keypass cisco
-keystore sds.keystore -storepass cisco
```

where the validity parameter specifies period of time in days during which the certificate is valid. For example, 3650 stands for 10 years.

g. Export the certificate by executing this command:

```
keytool -exportcert -alias sds -file C:\cert\sds.cer -keystore
sds.keystore -storepass cisco
```

The exported certificate is stored in *C:\cert\sds.cer*.

h. Import the certificate reply into the keystore using the same alias that was used when generating the certificate request. Assuming the file that is returned from the certificate authority or, if using self-signed certificate, the certificate exported from Cisco Unified Videoconferencing Desktop Server or Cisco Unified Videoconferencing Manager is c:\cert\cert.crt. Execute this command:

```
keytool -import -trustcacerts -alias <alias> -file C:\cert\cert.crt
-keystore <keystore> -storepass cisco
```

Configuring Mutual Authentication Using Certificates Generated by a CA

This procedure describes how to acquire a unique certificate using a CA, and then replace a default certificate on Cisco Unified Videoconferencing Desktop Server and Cisco Unified Videoconferencing Manager with a unique certificate.

Procedure

Step 1 Stop the appropriate service:

- For Cisco Unified Videoconferencing Desktop Server, "Desktop - Apache Tomcat"
- For Cisco Unified Videoconferencing Manager, "Cisco Cisco Unified Videoconferencing Manager"

Step 2 Locate the key store file:

- For Cisco Unified Videoconferencing Desktop Server, the key store is located at *<CUVCDINSTALLDIR>\data\sds.keystore*.
- For Cisco Unified Videoconferencing Manager, the key store is located at *<CUVCMINSTALLDIR>\iCM\jboss\server\default\conf\icmservice.keystore*.

Step 3 Copy the key store file to a temporary working folder, for example *C:\cert*.

Step 4 Open a command line window.

Step 5 Navigate to the JDK bin folder at this location:

- For Cisco Unified Videoconferencing Desktop Server, the bin folder is located at *<CUVCDINSTALLDIR>\JRE\bin*
- For Cisco Unified Videoconferencing Manager, the bin folder is located at *<CUVCMINSTALLDIR>\iCM\jre1.6.0_10\bin*

Step 6 Using the key tool utility, remove the default certificate from the sds.deystore file by entering this command:

- For Cisco Unified Videoconferencing Desktop Server, the command is:

  ```
  keytool -delete -alias default -keystore C:\cert\sds.keystore
  -storepass cisco
  ```

- For Cisco Unified Videoconferencing Manager, the command is:

  ```
  keytool -delete -alias default -keystore C:\cert\icmservice.keystore
  -storepass cisco
  ```

Step 7 Generate a private key using an appropriate DN:

- For Cisco Unified Videoconferencing Desktop Server, the command is:

```
keytool -genkeypair -keyalg RSA -alias sds -dname "CN=fully
qualified server name, OU=organization unit name, O=organization
name, L=location, ST=state, C=country" -keystore
C:\cert\sds.keystore -storepass cisco -validity NNNN -keysize 1024
-keypass
```

- For Cisco Unified Videoconferencing Manager, the command is:

```
keytool -genkeypair -keyalg RSA -alias cisco -dname "CN=fully
qualified server name, OU=organization unit name, O=organization
name, L=location, ST=state, C=country" -keystore
C:\cert\icmservice.keystore -storepass cisco -validity NNNN -keysize
1024 -keypass
```

where the validity parameter specifies period of time in days during which the certificate is valid. For example, 3650 stands for 10 years.

If you omit the keypass parameter value, the utility prompts you to provide it.

Note The store name and password are the default to Cisco Unified Videoconferencing Desktop Server. If alternate values are used, update the corresponding configuration properties in the [sslcontextfactory] section of the ctmx.ini file.

Step 8 Create a certificate request file for the private key pair generated in Step 7:

- For Cisco Unified Videoconferencing Desktop Server, the command is:

```
keytool -certreq -alias sds -keystore C:\cert\sds.keystore
-storepass cisco -file C:\cert\certreq.csr
```

- For Cisco Unified Videoconferencing Manager, the command is:

```
keytool -certreq -alias cisco -keystore
C:\cert\cuvcmrmservice.keystore -storepass cisco -file
C:\cert\certreq.csr
```

Step 9 Send the certificate request to a Certificate Authority.

Step 10 Import a trusted root certificate into sds.keystore file:

- For Cisco Unified Videoconferencing Desktop Server, the command is:

```
keytool -import -trustcacerts -alias root -file
C:\cert\root_cert.crt -keystore C:\cert\sds.keystore -storepass
cisco
```

- For Cisco Unified Videoconferencing Manager, the command is:

```
keytool -import -trustcacerts -alias root -file
C:\cert\root_cert.crt -keystore C:\cert\cuvcmrmservice.keystore
-storepass cisco
```

where <root_cert.crt> is the trusted root certificate.

Note Although you can use default certificates from the system default trusted certificate store, we recommend that you import a trusted root as described in this step. You cannot use default certificates for server authentication.

Step 11 The CA returns the certificate reply in form of .crt file, for example *C:\cert\cert.crt*.

Step 12 Import the Certificate reply into the sds.keystore file. Use the same alias you used in Step 8.

- For Cisco Unified Videoconferencing Desktop Server, the command is:

```
keytool -import -trustcacerts -alias sds -file C:\cert\cert.crt
-keystore C:\cert\sds.keystore -storepass cisco
```

- For Cisco Unified Videoconferencing Manager, the command is:

```
keytool -import -trustcacerts -alias cisco -file
C:\cert\root_cert.crt -keystore C:\cert\cuvcmrmservice.keystore
-storepass cisco
```

Upon completion this message is displayed: "Certificate reply was installed in keystore".

Note The trustcacerts parameter instructs the key tool utility to check the system key store while looking for the root certificate, if it is not present in the specified key store.

Step 13 Copy the key store file into its original location:

- For Cisco Unified Videoconferencing Desktop Server, the key store is located at *<CUVCDINSTALLDIR>\data\sds.keystore*.
- For Cisco Unified Videoconferencing Manager, the key store is located at *<CUVCMINSTALLDIR>\iCM\jboss\server\default\conf\icmservice.keystore*.

Step 14 Start the appropriate service:

- For Cisco Unified Videoconferencing Desktop Server, "Desktop - Apache Tomcat"
- For Cisco Unified Videoconferencing Manager, "Cisco Unified Videoconferencing Manager”.

Configuring Windows Firewall

Use the procedure described in this section to disable non-SSL access to Cisco Unified Videoconferencing Desktop Server and to enable secure connections to Cisco Unified Videoconferencing Desktop Server.

Note If Cisco Unified Videoconferencing Manager is installed on a separate server, Windows Firewall must be modified on both servers.

Procedure

Step 1 Open Windows Firewall by selecting **Start > Control Panel > Windows Firewall**.

Step 2 Select **On** to turn on firewall protection.

Step 3 Select the **Exceptions** tab.

Step 4 Select the **Add Port** button.

Step 5 Enter "Cisco Unified Videoconferencing Manager connection from" in the **Name** field.

Step 6 Enter 8080 in the **Port number** field.

Step 7 Verify that the TCP option is selected.

Step 8 Select **Change scope**.

Step 9 Select **Custom** list.

Step 10 Enter "127.0.0.1,<CUVCD IP address>" in the field, where <CUVCD IP address> represents the actual address of the Cisco Unified Videoconferencing Desktop Server. For example, "127.0.0.1,192.168.112.9".

Step 11 Select **OK**.

Step 12 Select **OK**.

Step 13 Select the **Advanced** tab.

Step 14 In the Network Connection Settings area, choose **Local Area Connection**, and then select **Settings**.

Step 15 Select **Secure Web Server (HTTPS)** to enable access to Cisco Unified Videoconferencing Desktop Server.

Step 16 Select **Add**.

Step 17 Define service settings:

a. In the Description field, enter Secure Cisco Unified Videoconferencing Manager.

b. In the Name or server address field, enter the name of the server.

c. In the External port number and Internal port number fields, enter 8444.

d. Verify that TCP is chosen.

e. Select **OK** to enable secure access to Cisco Unified Videoconferencing Manager.

Step 18 Select **OK**.

Step 19 Select **OK**.

Example of Using the Microsoft Certificate Service

This section provides an example of how to acquire a server certificate for Cisco Unified Videoconferencing Desktop Server using Microsoft Certificate Service application.

Configure Desktop When Using Microsoft CA

This section shows an example of replacing the Cisco Unified Videoconferencing Desktop Server certificate, when using Microsoft Certificate Service. You can replace the Cisco Unified Videoconferencing Manager certificate in a similar way.

Procedure

Step 1 Remove the default certificate from the keystore:

```
keytool -delete -alias default -keystore C:\cert\sds.keystore -storepass
cisco
```

Step 2 Download a CA certificate from *http://ca.server/certsrv/*, select Download a CA certificate, certificate chain, or CRL in DER format and save it as *C:\cert\root_cert.crt*.

Step 3 Import the CA certificate into your keystore:

```
keytool -import -trustcacerts -alias root -file C:\cert\root_cert. crt
-keystore C:\cert\sds.keystore -storepass cisco
```

Step 4 Generate a private key using an appropriate DN:

```
keytool -genkeypair -keyalg RSA -alias sds -dname " CN=fully qualified
server name, OU=organization unit name, O=organization name,
L=location, ST=state, C=country " -keystore C:\cert\sds.keystore
-storepass cisco
```

Step 5 Create a certificate signing request file for the private key generated in the previous step:

```
keytool -certreq -alias sds -keystore C:\cert\sds.keystore -storepass
cisco -file C:\cert\sds_certreq.csr
```

Step 6 Open sds_certreq.csr with Notepad and copy the content, and then request a certificate from *http://ca.server/certsrv/* by selecting the **Request a certificate link**:

- **a.** Select **Request** a certificate.
- **b.** Select **advanced certificate request** link.
- **c.** Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
- **d.** Paste content that you copied into the Saved Request field, choose Subordinate Certification Authority for the Certificate Template, and select **Submit**.

Step 7 Save it in *C:\cert\sds_cert.crt*.

Step 8 Import the certificate reply into the keystore:

```
keytool -import -trustcacerts -alias sds -file C:\cert\sds_cert.crt
-keystore C:\cert\sds.keystore -storepass cisco
```

Generating a PKCS12 Certificate Using Microsoft Certificate Service

Procedure

Step 1 Connect to the Certificate Authority Server at this link *http://<serverName>/certsrv.*

Step 2 On the Welcome Page select **Request a Certificate**.

Step 3 On the Request a Certificate page select advanced certificate request.

Step 4 On the Advanced Certificate Request page select Create and submit a request to this CA.

Step 5 On the Advanced Certificate Request page fill in the following information:

a. Certificate Template: Duplicate Computer

- Name: FQDN for the Server requesting the certificate

b. Key Options:

- CSP: Microsoft RSA SChannel Cryptographic Provider
- Key Usage: Exchange
- Key Size: 1024
- Automatic key container name
- Check Mark keys as exportable

c. Select **Submit**.

Step 6 If a Potential Scripting Violation warning appears, select **Yes** to request the Certificate.

Step 7 Select the **Install this certificate** link.

Step 8 If a Potential Scripting Violation warning appears, select **Yes** to request the Certificate.

Step 9 Verify that you receive a message stating that the certificate has been successfully installed.

Export the Certificate

Procedure

Step 1 Right-click the **Certificate** and select **All Tasks > Export**.

Step 2 Select **Next**.

Step 3 Select **Yes, export the private key**.

Step 4 Select Personal Information Exchange - PKCS #12 (.PFK).

Step 5 Also select **Include all certificates in the certification path if possible** option and **Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)**, then and select **Next**.

Step 6 Enter a password.

Step 7 Re-enter the password to confirm it.

Step 8 Select **Browse** and navigate to the location you would like to save the certificate to and enter a name and save. (Verify that it is saved as a .pfx file).

Step 9 Verify the information and select **Finish**.

Importing the Server Certificate into the Personal Certificate Store on the Local Computer

Procedure

Step 1 Right-click the Personal Store located under Certificates (Local Computer).

Step 2 Select **All Tasks > Import**, and then select **Next**.

Step 3 Select **Browse**, and then select the **Certificate**.

Note By default it only shows X.509 Certificate file types, you must change this to Personal Information Exchange (*.pfx;*.p12) or All Files (*.*).) and select Next.

Step 4 Enter the password and select the **Mark this key as exportable** check box, and then select **Next**.

This will allow you to back up or transport your keys at a later time.

Step 5 Verify that Place all certificates in the following store > Certificate store: Personal is selected.

Step 6 Select **Next**.

Step 7 Verify the information and select **Finish**.

APPENDIX B

Configuring Dual-NIC Cisco Unified Videoconferencing Solution Deployments

- About the Functionality of Dual-NIC Deployments, page B-1
- Using Cisco Unified Videoconferencing Desktop Server in Dual-NIC Deployments, page B-2
- Configuring Settings for Dual/Single-NIC Deployments, page B-3

About the Functionality of Dual-NIC Deployments

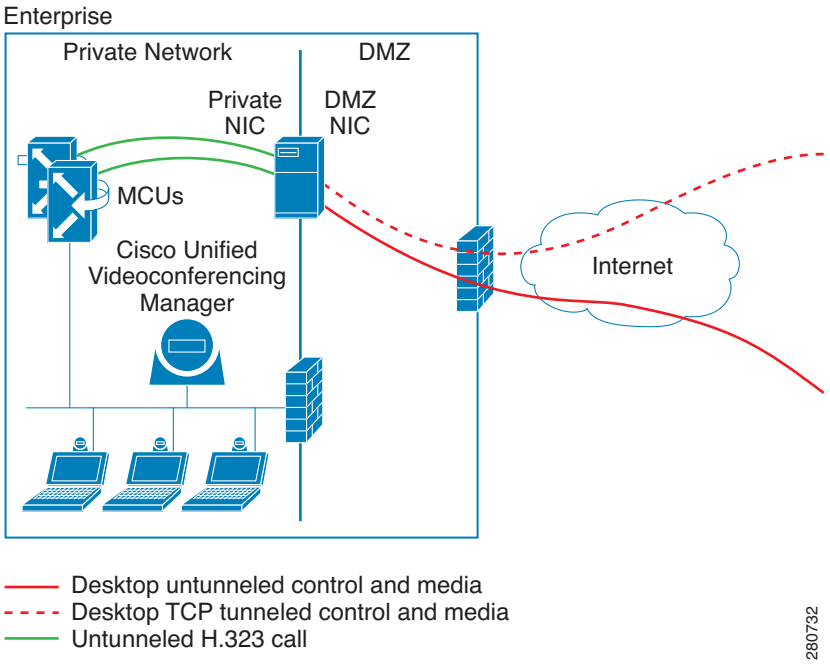
This chapter provides general information about the dual-NIC deployment of the Cisco Unified Videoconferencing Desktop Server component of the Cisco Unified Videoconferencing Manager and its configuration. Dual-NIC deployments provide a simpler network configuration as well as better security. Dual-NIC deployments are more secure, since ports between a DMZ and a private network do not need to be opened for Cisco Unified Videoconferencing Desktop Server. Dual-NIC deployments allow you to bridge the internal firewall. External client access is only granted to the external NIC. The internal NIC communicates with the internal network components (Cisco IOS H.323 Gatekeeper, Cisco Unified Videoconferencing 3500 MCU, and Cisco Unified Videoconferencing Manager) and internal clients.

Each of the two NICs is assigned to a separate IP address according to its IP network range. You must use an FQDN with DNS resolution on the private network for the internal IP and external IP on the extranet.

Note In large centralized deployments which use a load balancer, we recommend that you use the dual-NIC deployment.

If your Cisco Unified Videoconferencing Desktop Server has dual-NIC cards, one of the NICs resides in the enterprise network and the other NIC resides in the DMZ, as shown in Figure B-1.

Figure B-1 Small Deployment—Dual NICs



Using Cisco Unified Videoconferencing Desktop Server in Dual-NIC Deployments

- Installing Cisco Unified Videoconferencing Desktop Server with Dual-NIC, page B-2
- Limiting Available IP Addresses in a Dual-NIC Deployment, page B-3

Installing Cisco Unified Videoconferencing Desktop Server with Dual-NIC

Procedure

Step 1 Perform the installation as described in Installing Cisco Unified Videoconferencing Desktop Server, page 2-6.

Step 2 During the installation, enter the private NIC address in the Cisco Unified Videoconferencing Desktop Server network interface address field.

Limiting Available IP Addresses in a Dual-NIC Deployment

Procedure

Step 1 Open the registry.

Step 2 Select **HKEY_LOCAL_MACHINE > SOFTWARE > Click To Meet > Conference Server > 7.xxx.xxx > Interfaces**.

The value of the registry key contains a list of IP addresses available for client connections to this Cisco Unified Videoconferencing Desktop Server. The addresses are separated by a space.

Step 3 Edit the list of addresses as required.

Step 4 Save the registry and close.

Step 5 Stop the Desktop Conference Server.

Step 6 Start the Desktop Conference Server.

Note Since the number of network cards may change between upgrades, these edits are not preserved during the upgrade procedure.

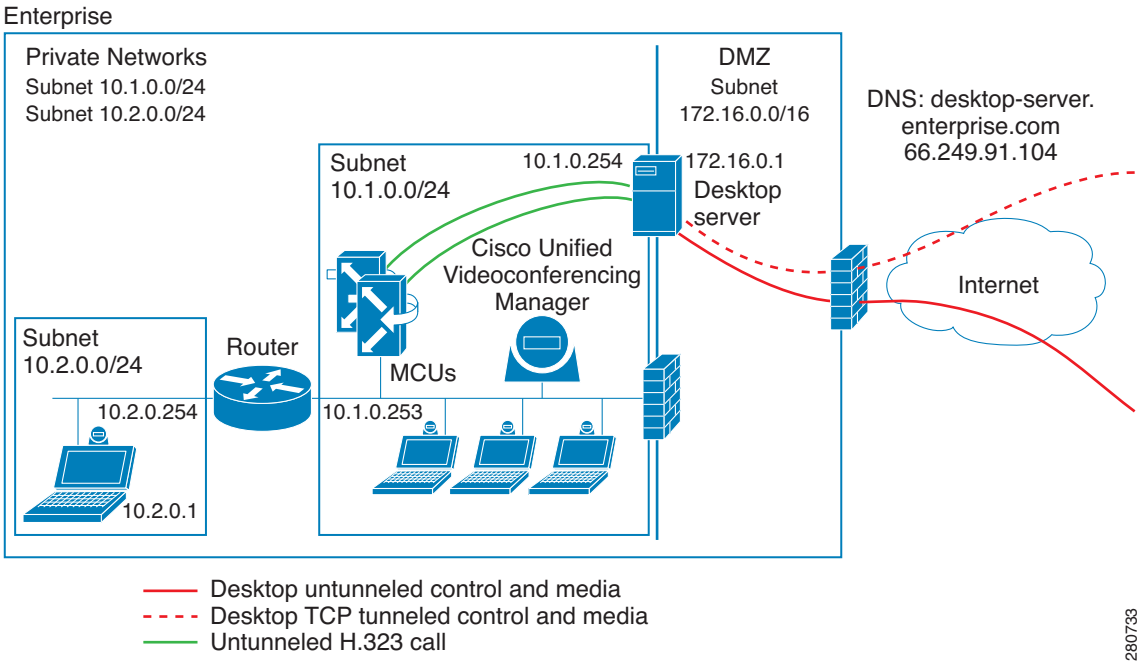
Configuring Settings for Dual/Single-NIC Deployments

- Deployment Examples, page B-4
- Configuring Cisco Unified Videoconferencing Desktop Server Network Interface, page B-5
- Modifying Static Routing Configuration, page B-5

Deployment Examples

Typically a corporate private network is comprised of several IP subnets, each having its own IP range as shown in Figure B-2. Routers provide an access to the subnets; in the presented example subnets have the following ranges: 10.1.0.0/24 and 10.2.0.0/24.

Figure B-2 Dual-NIC Deployment Example



The Cisco Unified Videoconferencing Desktop Server can have multiple Network Interface Cards (NICs). Depending on the deployment and network configuration, you might want to control which NIC is used for various server communications.

In secure multiple NIC deployments you can use a NIC configured behind the firewall to communicate with various servers, while using another NIC to which the external Desktop Clients connect. You must configure the Cisco Unified Videoconferencing Desktop Server network interface address to represent the NIC behind the firewall. Then in the Public Address (FQDN) field on the Servers tab, enter a DNS name which resolves to the NIC outside the firewall and is accessible both inside and outside the corporate network. In the example presented in Figure B-2, the NIC for external Desktop Clients connection is 172.16.0.1, the NIC behind the firewall is 10.1.0.254, FQDN is desktop-server.enterprise.com, and the address 66.249.91.104 is statically mapped to 172.16.0.1.

FQDN represents the Cisco Unified Videoconferencing Desktop Server IP address which both internal and external clients use for connection.

Desktop Clients can connect to the Cisco Unified Videoconferencing Desktop Server either by an IP or a DNS name. If a DNS name is not specified in the Public Address field, the Cisco Unified Videoconferencing Desktop Server network interface address is used. However, in many deployments the Cisco Unified Videoconferencing Desktop Server network interface address is not accessible to clients outside the intranet, due to NAT or firewall restrictions. Therefore, we recommend that you specify the Public Address, which must be a DNS name resolving to the correct Cisco Unified Videoconferencing Desktop Server IP address both inside and outside the corporate network. In the example presented in Figure B-2, the FQDN: desktop-server.enterprise.com is resolved to 64.233.187.99 for external clients and to 10.1.0.254 for internal clients.

Configuring Cisco Unified Videoconferencing Desktop Server Network Interface

This section describes how to configure a network interface address for the Cisco Unified Videoconferencing Desktop Server. The Cisco Unified Videoconferencing Desktop Server communicates with the following types of servers in the deployment:

- Cisco Unified Videoconferencing 3500 MCU and Cisco Unified Videoconferencing 3500 MCU—For media and call setup.
- Cisco Unified Videoconferencing Manager or Cisco Unified Videoconferencing 3500 MCU—For moderation and meeting control.
- Cisco Unified Videoconferencing Streaming Server—For media and control.

Procedure

Step 1 Select **Status** in the sidebar of the Cisco Unified Videoconferencing Desktop Server, and then select the link showing the Cisco Unified Videoconferencing Desktop Server IP address.

Step 2 Enter the IP address that the Cisco Unified Videoconferencing Desktop Server must use to communicate with various servers.

Note The light next to the **Address** field indicates whether connection to the Cisco Unified Videoconferencing Desktop Server is successful or not. When the light is red, a tooltip containing error details is displayed.

Step 3 For secure multiple NIC deployments, enter a DNS name in the **Public Address** field.

Step 4 Select the maximum call rate from the list.

Step 5 Select **OK** or **Apply**.

Modifying Static Routing Configuration

You must perform the procedure described in this section only for IP subnets located behind routers in a private network. Do not modify the static routing configuration for a private network subnet used by the Cisco Unified Videoconferencing Desktop Server. For example, for a deployment illustrated in Figure B-2 on page B-4, do not modify the static routing configuration for subnet 10.1.0.0/24.

Procedure

Step 1 Open the Windows command line window.

Step 2 Enter:

```
route add <IP subnet> mask <subnet mask> <router IP address> -p
```

For example,

```
route add 10.2.0.0 mask 255.255.255.0 10.1.0.253 -p
```

Step 3 Perform Step 2 for all IP subnets located behind routers.

APPENDIX C

Configuring the Cisco Unified Videoconferencing Manager Prefix

A virtual room prefix consists of a Cisco Unified Videoconferencing Manager prefix and a user ID. For example, if the Cisco Unified Videoconferencing Manager prefix is 68 and a user ID is 6209, this user's virtual room number is automatically set to 686209.

Note The Cisco Unified Videoconferencing Manager prefix is unique for every Cisco Unified Videoconferencing Solution system.

You might need to change the Cisco Unified Videoconferencing Manager prefix for the following reasons:

- To avoid a collision with existing meeting types (MCU or Gateway service IDs)
- To avoid a collision with existing H.323 room system numbers

Procedure

Step 1 In an internet browser, enter the following address:

http://<your server IP>:8080/cuvcmrm-config

Step 2 Select **Launch Configuration Tool**. in the Resource Manager Configuration Tool window.

Step 3 If the Security window opens, select **Run**.

Step 4 Enter the administrator's login ID and password in the Resource Manager Configuration Tool window, and then select Login.

Note The default administrator's login ID is "admin". No password is necessary by default.

Step 5 Select the **Scheduling Settings** tab in the Cisco Unified Videoconferencing Manager Configuration Tool window.

Step 6 Change a value in the Meeting ID Prefix field.

Step 7 Select **Save**.

Step 8 Select **Yes** to confirm the change.

Step 9 Select **Close** in the Cisco Unified Videoconferencing Manager Configuration Tool window.

Step 10 Select **Yes**.

Step 11 Close the Resource Manager Configuration tool.

APPENDIX D

Configuring a Firewall

- Firewall Rules, page D-1
- NAT Rules, page D-5

Firewall Rules

This section describes firewall rules used for the simplest and most typical firewall configuration.

Table D-1 presents general firewall rules that comply with the guidelines described in Firewall Guidelines, page 3-28.

Table D-1 General Firewall Rules

Action	Protocol	Source	Port	Destination	Port	Description
Pass	Any	LAN networks	Any	DMZ net, outside networks	Any	Allowing any kind of traffic from the private network to the DMZ or outside networks (for example the Internet).
Block	Any	Outside networks	Any	LAN networks, DMZ network	Any	Blocking any kind of traffic to the protected networks (DMZ and internal network).
Block	Any	DMZ network	Any	LAN networks	Any	Blocking any kind of traffic from the DMZ to the private network.

Table D-2 describes rules that you must add to enable connectivity between the Internal Cisco IOS H.323 Gatekeeper located in the DMZ, and the MCU and MVP components located on the internal network.

Table D-2 Gatekeeper-to-MCU Traffic Firewall Rules

Action	Protocol	Source	Port	Destination	Port	Description
Pass	TCP	Cisco IOS H.323 Gatekeeper IP address as it appears in the DMZ	Any	MCU IP address(es)	1025 - 65535	TCP High ports from Cisco IOS H.323 Gatekeeper to MCU on the LAN. Enables H.245 control signaling channels to be opened.
Pass	TCP	Cisco IOS H.323 Gatekeeper IP address as it appears in the DMZ	Any	MCU IP address(es)	2720	H.323 signaling to MCU on the LAN. Enables call setup signaling between the internal Cisco IOS H.323 Gatekeeper and the MCU(s).

Table D-3 describes rules that you must add to enable connectivity between the internal Cisco Unified Videoconferencing Manager located in the DMZ and the Cisco Unified Videoconferencing 3500 MCU located on the internal network.

Table D-3 Cisco Unified Videoconferencing Manager-to-MCU Traffic Rules

Action	Protocol	Source	Port	Destination	Port	Description
Pass	TCP	Cisco Unified Videoconferencing Manager IP address as it appears in the DMZ	Any	Cisco Unified Videoconferencing Desktop Server IP address(es)	3340	Login (XML) to MCU on the LAN. Enables XML management interface connectivity between the Cisco Unified Videoconferencing Manager and the Cisco Unified Videoconferencing Desktop Server.
Pass	UDP	Cisco Unified Videoconferencing Manager IP address as it appears in the DMZ	Any	Cisco Unified Videoconferencing 3500 MCU IP address(es)	161	SNMP from Cisco Unified Videoconferencing Manager to Cisco Unified Videoconferencing 3500 MCU on the LAN. Enables SNMP management interface connectivity between the Cisco Unified Videoconferencing Manager and the Cisco Unified Videoconferencing 3500 MCU component(s).

Table D-4 describes a rule that you must add to enable connectivity between the internal Cisco IOS H.323 Gatekeeper located in the DMZ and Cisco Unified Videoconferencing 3545 Gateway component(s) located on the private network.

Table D-4 Cisco IOS H.323 Gatekeeper-to-gateway Traffic Firewall Rules

Action	Protocol	Source	Port	Destination	Port	Description
Pass	TCP	Cisco IOS H.323 Gatekeeper IP address as it appears in the DMZ	Any	Cisco Unified Videoconferencing 3545 Gateway IP address(es)	1025 - 65535	TCP High ports from Cisco IOS H.323 Gatekeeper to GW320 on the LAN. Enables H.245 control signaling channels to be opened.

Table D-5 describes rules that you must add to enable a Desktop Client to invite a room system located on the private network.

Table D-5 Gatekeeper-to-endpoint Traffic Firewall Rules

Action	Protocol	Source	Port	Destination	Port	Description
Pass	TCP	Cisco IOS H.323 Gatekeeper IP address as it appears in the DMZ	Any	Room system IP address(es) as it appears on the private network	1720	H.323 signaling to a room system on the LAN. Enables call setup signaling between the internal Cisco IOS H.323 Gatekeeper and room systems.
Pass	TCP	Cisco IOS H.323 Gatekeeper IP address as it appears in the DMZ	Any	Room system IP address(es) as it appears on the private network	1025 - 65535	TCP High ports from Cisco IOS H.323 Gatekeeper to room system on the LAN. Enables H.245 control signaling channels to be opened.

Table D-6 describes rules that must be added to enable connectivity between the internal Cisco Unified Videoconferencing Manager located in the DMZ and MCU component/s located on the internal network.

Table D-6 Cisco Unified Videoconferencing Manager-to-gateway Traffic Firewall Rules

Action	Protocol	Source	Port	Destination	Port	Description
Pass	TCP	Cisco Unified Videoconferencing Manager IP address as it appears in the DMZ	Any	GW IP address(es)	1820	H.323 Signaling from Cisco IOS H.323 Gatekeeper to GW320 on the LAN. Enables call setup signaling between the internal Cisco IOS H.323 Gatekeeper and the Cisco Unified Videoconferencing 3545 Gateway(s).
Pass	UDP	Cisco Unified Videoconferencing Manager IP address as it appears in the DMZ	Any	GW IP address(es)	161	SNMP from Cisco Unified Videoconferencing Manager to gateway on the LAN. Enables SNMP management interface connectivity between the Cisco Unified Videoconferencing Manager and the gateway component(s).

Table D-7 describes rules that you must add to enable connectivity between the internal Cisco Unified Videoconferencing Manager located in the DMZ and the MCU components located on the internal network.

Table D-7 Desktop-to-MCU Traffic Firewall Rules

Action	Protocol	Source	Port	Destination	Port	Description
Pass	UDP	Cisco Unified Videoconferencing Manager IP address as it appears in the DMZ	Any	Cisco Unified Videoconferencing Desktop Server IP address(es)	10000 - 65535	Media connection between the Desktop and MCU. Also open ports between the Cisco Unified Videoconferencing Desktop Server and the EMP. To avoid a conflict with SIP traffic, limit the port range by setting the value opening the range to 10,000 or higher. For operational information about configuring ports, see the *Configuration Guide for Cisco Unified Videoconferencing Manager*.
Pass	UDP	Desktop	Any	MCU	10000-65535	Limit UDP ports opened on the firewall to allow Desktop to send RTP to the internal network (MCU). We recommend that you use a limited range between 10000 and 65535. If this option is used: • Each Client-to-Desktop connection uses 2 UDP ports. • Each Cisco Unified Videoconferencing Desktop Server-to-MCU connection uses UDP ports. Reserve 11 ports per user. To define the range, multiply the number of connections allowed by your license by 11. In addition, 6 UDP ports each are required for: • Every conference with Desktop users. • Every recording channel.

Note The range of UDP ports opened on the firewall can be limited further in the Desktop Administration Utility.

NAT Rules

Table D-8 describes static NAT entries in the firewall WAN interface that you must configure to enable connectivity between Desktop Clients located on the external networks and Cisco Unified Videoconferencing Desktop Server(s) located in the DMZ.

Table D-8 NAT Rules defining traffic from Desktop Clients to Web Services

Protocol	External Port Range	NAT IP	Internal Port Range	Description
TCP	80 (HTTP)	Cisco Unified Videoconferencing Desktop Server IP address as it appears in the DMZ	80 (HTTP)	For external Desktop Client web access. Alternatively the Desktop Clients can be configured to connect via TCP port 443. For more information about configuring TCP port 443, see Appendix A, "Configuring Secure Connection Between Cisco Unified Videoconferencing Solution Components".
TCP	443 (HTTPS)	Cisco Unified Videoconferencing Desktop Server IP address as is appears in the DMZ	443 (HTTPS)	Control connection between Cisco Unified Videoconferencing Desktop Server and Desktop Client (mandatory).
TCP	8080	Cisco Unified Videoconferencing Manager Cisco Unified Videoconferencing Desktop Server IP address as is appears in the DMZ	8080	For external Desktop Client web access to a virtual room configuration. Enables Desktop Client access to Cisco Unified Videoconferencing Manager virtual room settings.

Table D-9 describes a static NAT entry in the firewall WAN interface that you must add to enable connectivity between Desktop Web Cast clients located on the external networks and Streaming Server located in the DMZ.

Table D-9 NAT Rules defining traffic from Desktop Webcast Clients to the Cisco Unified Videoconferencing Streaming

Protocol	External Port Range	NAT IP	Internal Port Range	Description
TCP	7070	Cisco Unified Videoconferencing Streaming Server IP as appears in the DMZ	7070	Streaming tunneling connection enables the Web Cast client to access the streamed conference.

Table D-10 describes a static NAT entry in the firewall WAN interface that you must add to enable connectivity between Desktop Web Cast clients located on the external networks and Cisco Unified Videoconferencing Streaming Server located in the DMZ.

Table D-10 NAT Rules defining traffic from Desktop Webcast Clients to the Cisco Unified Videoconferencing Desktop Server

Protocol	External Port Range	NAT IP	Internal Port Range	Description
UDP	Any	Cisco Unified Videoconferencing Desktop Server IP as appears on the DMZ	10000-65535	Media connection between the Desktop Client and Cisco Unified Videoconferencing Desktop Server. If not open, the connection will be tunneled via TCP port 443 effecting performance. To avoid a conflict with SIP traffic, limit the port range by setting the value opening the range to 10,000 or higher. For operational information about configuring ports, see *Configuration Guide for Cisco Unified Videoconferencing Manager*.