CISCO SYSTEMS

Administrator's Guide for Cisco IPVC 3511 MCU and Cisco IPVC 3540 MCU Module

Releases 4.0, 4.1, and 4.2
January 2006

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Administrator's Guide for Cisco IPVC 3511 MCU and Cisco IPVC 3540 MCU Module Releases 4.0, 4.1, and 4.2

CONTENTS

Preface

This preface describes the objectives, intended audience, and organization of the *Administrator's Guide for Cisco IPVC 3511 MCU and Cisco IPVC 3540 MCU Module Releases 4.0, 4.1, and 4.2* and defines the conventions used to convey instructions and information. It also discusses how to obtain documentation and technical support.

Objectives

This guide describes how to install, configure, and use the Cisco IPVC 3511 MCU and the Cisco IPVC 3540 MCU module.

Audience

This guide is intended for:

- Network administrators who need instructions about how to install and configure the Cisco IPVC 3511 MCU and the Cisco IPVC 3540 MCU module as well as create conferences using the Administrator interface.

- Users who create and manage conferences using the Conference Control interface.

⚠

Warning   **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.**

⚠

Warning   **This unit is intended for installation in restricted access areas. A restricted access area is where access can only be gained by service personnel through the use of a special tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.**

⚠

Warning   **Read the installation instructions before you connect the system to its power source.**

⚠

Warning   **The device is designed to work with TN power systems.**

Document Organization

Table 1 provides an overview of the organization of this guide.

Table 1   Administrator's Guide for Cisco IPVC 3511 MCU and Cisco IPVC 3540 MCU Module Organization

Chapter	Description
Chapter 1, "Overview of the Cisco IPVC 35xx MCU"	Provides a general overview of Cisco IPVC 35xx MCU products, features, and network architecture.
Chapter 2, "Installing the Cisco IPVC 35xx MCU"	Describes how to install the Cisco IPVC 3511 MCU and Cisco IPVC 3540 MCU Module, how to use the Administrator interface to configure board settings and add Cisco IPVC 35xx MCU users.
Chapter 3, "Configuring the Cisco IPVC 35xx MCU"	Describes how Administrators can create conferences using the Administrator interface.
Chapter 4, "Using the Cisco IPVC 35xx MCU"	Describes how Administrators, Operators, and Users can create or join conferences from endpoints or by using the Conference Control interface.
Chapter 5, "Troubleshooting the Cisco IPVC 35xx MCU"	Provides troubleshooting information for the Cisco IPVC 35xx MCU.

Scope

The *Administrator's Guide for Cisco IPVC 3511 MCU and Cisco IPVC 3540 MCU Module Releases 4.0, 4.1, and 4.2* contains information about installing and upgrading the software for the Cisco IPVC 3511 MCU and Cisco IPVC 3540 MCU module.

Note   This document was previously titled *Cisco IPVC 3511 MCU and Cisco IPVC 3540 MCU Module Administrator's Guide* Release 4.0.

Naming Conventions Used in This Guide

Table 2 lists the naming conventions used in this guide.

Table 2   Naming Conventions

Product	Convention
Cisco IPVC 3511 MCU and Cisco IPVC 3540 MCU module	Cisco IPVC 35xx MCU
Cisco IPVC 3540 Rate Matching Module	Rate Matching Module (RMM)
Cisco IPVC 3540 Application Server (AS) Module for Data Collaboration Server (DCS)	Data Collaboration Server (DCS)

Document Conventions

Table 3 lists the conventions that Cisco IPVC 35xx MCU documentation set uses.

Table 3   *Document Conventions*

Convention	Description
>	Indicates movement through menu options, for example: Click **Start > Run.**
boldface	Indicates a button that you are instructed to click, for example: Click **Next.**
`screen`	Shows an example of information displayed on the screen.
`boldface screen`	Shows an example of information that you must enter.

Command Syntax Conventions

Table 4 lists the conventions that command descriptions use.

Table 4   *Command Syntax Conventions*

Convention	Description
boldface	Indicates commands and keywords that are entered literally as shown.
italics	Indicates arguments for which you supply values; in contexts that do not allow italics, arguments are enclosed in angle brackets ($< >$).
[**x**]	Indicates optional keywords or arguments.
{**x** | **y** | **z**}	Indicates a choice of required keywords (represented by **x**, **y**, and **z**). You must select one.
[**x** {**y** | **z**}]	Indicates a required choice within an optional element. You do not need to select keyword **x**, but if you do, you must specify either argument **y** or argument **z**.

The following conventions are used to attract the reader's attention:

Note   Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution   Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning   This warning symbol means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.

Waarschuwing   Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het document *Regulatory Compliance and Safety Information* (Informatie over naleving van veiligheids- en andere voorschriften) raadplegen dat bij dit toestel is ingesloten.

Varoitus   Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. Tässä julkaisussa esiintyvien varoitusten käännökset löydät laitteen mukana olevasta *Regulatory Compliance and Safety Information* -kirjasesta (määräysten noudattaminen ja tietoa turvallisuudesta).

Attention   Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions d'avertissements figurant dans cette publication, consultez le document *Regulatory Compliance and Safety Information* (Conformité aux règlements et consignes de sécurité) qui accompagne cet appareil.

Warnung   Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Dokument *Regulatory Compliance and Safety Information* (Informationen zu behördlichen Vorschriften und Sicherheit), das zusammen mit diesem Gerät geliefert wurde.

Avvertenza   Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nel documento *Regulatory Compliance and Safety Information* (Conformità alle norme e informazioni sulla sicurezza) che accompagna questo dispositivo.

Advarsel	Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du vare oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i dokumentet *Regulatory Compliance and Safety Information* (Overholdelse av forskrifter og sikkerhetsinformasjon) som ble levert med denne enheten.
Aviso	Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. Para ver as traduções dos avisos que constam desta publicação, consulte o documento *Regulatory Compliance and Safety Information* (Informação de Segurança e Disposições Reguladoras) que acompanha este dispositivo.
¡Advertencia!	Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. Para ver una traducción de las advertencias que aparecen en esta publicación, consultar el documento titulado *Regulatory Compliance and Safety Information* (Información sobre seguridad y conformidad con las disposiciones reglamentarias) que se acompaña con este dispositivo.
Varning!	Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. Se förklaringar av de varningar som förkommer i denna publikation i dokumentet *Regulatory Compliance and Safety Information* (Efterrättelse av föreskrifter och säkerhetsinformation), vilket medföljer denna anordning.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only — security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

    http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

    http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

    http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

    http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

1

Overview of the Cisco IPVC 35xx MCU

Revised: January 2006, OL-7777-03
This chapter describes the following topics:

About the Cisco IPVC 35xx MCU

The Cisco IPVC 35xx MCU is a high performance multipoint video conferencing and media processing system that provides extensive audio and video processing capabilities and web-based conference monitoring and management. The Cisco IPVC 35xx MCU supports a wide range of telephony protocols and media communication networks and is fully interoperable with other video conferencing network devices.

The Cisco IPVC 35xx MCU supports a range of features to enhance the video conferencing user experience. A user interacts with the Cisco IPVC 35xx MCU in three ways:

- Administrator interface—The Administrator uses this to manage and configure the Cisco IPVC 35xx MCU.
- Conference Control interface—Users use this to view conference details and manage different aspects of a conference.
- Video or audio conference—This is the actual video or audio conference.

About Videoconferencing

Videoconferencing using the H.323 protocol enables users of personal computers, IP telephones, and room systems to communicate across the office and around the world over IP networks. Spurred by changes in communications technology, low-cost bandwidth, and continuous improvements in hardware and performance, videoconferencing solutions provide the tools that large and small enterprises, government institutions, and educational environments need for greater productivity, faster decision making, more efficient training and education, and to save time and avoid the burden of travel.

About the H.323 Standard

The International Telecommunication Union (ITU) created the H.323 standard for real-time audio, data, and video communication over packet-based Internet Protocol (IP) networks. The H.323 standard defines basic components used in IP-based videoconferencing systems. These components include:

* Multipoint Control Unit (MCU): An H.323 endpoint that enables the capacity for three or more terminals and gateways to participate in multipoint conferences. An MCU has two components: multipoint controller (MC) and multipoint processor (MP).

  The MC is the conference controller. It sets and communicates call parameters to each participating endpoint and controls videoconference resources such as multicasting. The MC does not process media streams.

  The MP processes media streams. It receives audio and video information from the endpoints for which it does the required mixing, switching, and other processing before distributing streams to the videoconference participants.

* Gateway: An H.323 component that enables protocol translation and enables LAN-based H.323 endpoints and Integrated Services Digital Network (ISDN)-based H.320 terminals to participate in the same videoconferences.

* Terminal: An H.323 endpoint that enables real-time, two-way communication with another H.323 terminal, gateway, or multipoint control unit. H.323 terminals can be desktop computers running H.323-compliant software or H.323-compatible IP phones. Terminals can support audio, video, and data communications. All terminals must support audio.

* Gatekeeper: A central component for many H.323 videoconference calls. A gatekeeper performs access control, address resolution, and bandwidth management. Some gatekeepers such as the Cisco IOS Gatekeeper also provide IP-IP gatekeeper support. This support performs network security and Quality of Service (QoS) capability for videoconference calls.

* When gatekeepers are installed on the network, all H.323 endpoints must register with a gatekeeper. The gatekeeper can facilitate peer-to-peer dialing between terminals and is required for multiparty calls and calls that include ISDN terminals. A gatekeeper and the endpoints that register with it constitute a zone.

About Cisco IPVC 35xx MCU Videoconferencing Products

Cisco IPVC 35xx MCU products provide H.323 videoconferencing solutions to suit the needs of different network environments. The series includes stand-alone devices designed for small and medium-size networks and chassis-based modules for large networks. The series offers MCUs, PRI and

BRI gateways, a Data Collaboration Server, a Rate Matching Module (RMM), an Enhanced Media Processor (EMP), and a web-based user interface. These devices are designed to interoperate. You can use stand-alone devices and chassis-based devices with each other.

About Stand-alone Devices

Stand-alone devices are self-contained units (such as the Cisco IPVC 3511 MCU) that are encased in a chassis that you can mount in a 19-inch rack. Table 1-1 briefly describes the other available Cisco IPVC 3500 stand-alone devices.

Table 1-1   Stand-alone Devices

Device	Description
Cisco IPVC 35xx MCU	Basic device with MC and MP components but without EMP support.
Cisco IPVC 3511 MCU and EMP	A Cisco IPVC 3511 MCU with a Cisco IPVC 3540 EMP module enclosed. These devices are independent in this configuration, but share a common power bus. You can use the Cisco IPVC 3540 EMP module with any Cisco IPVC 35xx MCU in your environment
Cisco IPVC 3521 BRI Gateway	Performs H.320–to–H.323 protocol translation to enable Public Switched Telephone Network (PSTN) endpoints to communicate with H.323 endpoints on the LAN. The BRI Gateway includes the following features: • Ports for four ISDN BRI lines • B-channel bonding up to 512 Kbps • Pass-through support for G.722 audio and H.263 video codecs • Audio transcoding • Interactive Voice Response (IVR) for incoming calls • Pass-through support for T.120 data collaboration
Cisco IPVC 3526 PRI Gateway	Performs H.320–to–H.323 protocol translation to enable Public Switched Telephone Network (PSTN) endpoints to communicate with H.323 endpoints on the LAN. The PRI Gateway includes the following features: • One port that accepts either a T1 or E1 ISDN line • B-channel bonding up to 1920 Kbps • Pass-through support for G.722 audio and H.263 video codecs • Audio transcoding • Interactive Voice Response (IVR) for incoming calls • Pass-through support for T.120 data collaboration

About Chassis-based Devices

The Cisco IPVC 3540 series is a chassis-based solution that provides increased scalability to accommodate large organizations. The Cisco IPVC 3544 chassis is 3.5-inches high and can mount in a 19-inch rack. It has a cPCI bus and can accommodate four Cisco IPVC 3540 modules (one module features controls for the bus). Table 1-2 briefly describes chassis-based devices.

Table 1-2   Chassis-based Devices

Device	Description
Cisco IPVC 3540 MCU Module	MCU module that installs in an Cisco IPVC 3544 chassis.
Cisco IPVC 3540 PRI Gateway	Performs H.320–to–H.323 protocol translations that allows PSTN endpoints to communicate with H.323 LAN endpoints. This devices has two PRI ports that support up to 46 B-channels on T1 networks or 60 B-channels for E1 networks. This card can provide controls for the cPCI bus in the chassis.
Cisco IPVC 3540 EMP and Cisco IPVC 3540 EMP 3	Dedicated media processor that supports up to three video bandwidths in a conference, layouts for up to 16 frames in continuous-presence displays, and displays participant information in frame.
Cisco IPVC 3540 T.120 Data Collaboration Server	Performs the processing that allows Cisco IPVC 35xx MCUs to provide data collaboration using white boards, spreadsheets and other tools in conference calls.

Table 1-2   Chassis-based Devices

Device	Description
Cisco IPVC 3540 Rate Matching Module	Performs the processing that enables Cisco IPVC 35xx MCUs to support two video bandwidths in a videoconference. When an endpoint does not support the video bandwidth specified in the conference service, the Cisco IPVC 35xx MCU only sends it the conference audio. The Rate Matching Module allows the Cisco IPVC 35xx MCU to offer a second and lower video bandwidth in the call for endpoints that do not support the higher bandwidth. The Rate Matching Module provides the Cisco IPVC 35xx MCU with a copy of the video stream received from the endpoint at the other bandwidth. This gives the Cisco IPVC 35xx MCU copies of the stream at both bandwidths to distribute to conference participants.
	The Rate Matching Module also enables the expansion of the number of participants (up to 16) in Continuous Presence conferences.

About the Web-Based User Interface

The Cisco IPVC 35xx MCU products have a web-based user interface. This serves as a single point of entry for configuring, controlling, and monitoring the Cisco IPVC 35xx MCU unit and conference sessions.

The Administrator interface provides authorized users with a comprehensive suite of control features for configuring, controlling, and managing the Cisco IPVC 35xx MCU unit, conference services, and supporting devices and applications. The Administrator interface also features remote device monitoring and configuration, as well as conference control from any location using a Java-enabled web browser.

The Conference Control interface displays conference and participant details and provides a comprehensive set of advanced control features for authorized users. Advanced control features allow audio, video, and data connection management, advanced conference view image positioning options, multiple layout selection and options for creating new conferences and sub-conferences.

About Cisco IPVC 35xx MCU Features

Table 1-3 lists all the main features of the Cisco IPVC 35xx MCU.

Table 1-3 **Cisco IPVC 35xx MCU Feature Summary**

Feature	Description
Supported protocols	• H.281 • H.235 • H.239 • H.320 • H.323 version 4 • Session Initiation Protocol (SIP) • Skinny Client Control Protocol (SCCP) • T.120
Audio transcoding codecs	Optional Transcoding Module (TCM) with Digital Signal Processing (DSP) devices performs audio transcoding for translating an audio stream in a video call from one codec type to another. The Cisco IPVC 35xx MCU supports the following audio transcoding codecs: • G.711 A/μ Law • G.723.1 • G.722 • G.728 • G.722.1 • G.729 A
Video coding	The Cisco IPVC 35xx MCU supports the following video coding: • H.261, H.263 and H.263+ and H.264 video formats in the same conference (requires EMP support). • H.264 in voice-activated mode without video transcoding. • H.264 in Continuous Presence mode (with EMP only). • Standard dual-video capability according to the H.239 protocol.
Video formats	The Cisco IPVC 35xx MCU supports the following video resolutions: • CIF, QCIF, 4CIF • SIF, 4SIF • VGA, SVGA, XGA

Table 1-3   ***Cisco IPVC 35xx MCU Feature Summary***

Feature	Description
Video processing support	Advanced video processing support using the Rate Matching Module (RMM) and Enhanced Media Processor (EMP) video enables conferences to accommodate multiple connection speeds participants simultaneously for each conference. The EMP also enables conference views and text overlays on the conference images.

Video switching modes	The Cisco IPVC 35xx MCU voice-activated full screen video switching with the following viewing options:
	
	• All see one. Only the active speaker appears.
	
	  – See you, see me. The active speaker can see the previous speaker or their own image.
	
	• Continuous Presence (CP) mode. The CP image, called a layout, is a composite of incoming participant video images. The range of available video layouts depends on the type of media processing your network supports. The following options are available:
	
	  – All Cisco IPVC 35xx MCUs support four CP, displaying a screen of four quadrants of equal size, each displaying the video image of a different participant.
	
	  – With Rate Matching Module or Enhanced Media Processor support, the Cisco IPVC 35xx MCU can support up to 16 participants simultaneously on the same screen.
	
	  – Zoom to highlight the current speaker.
	
	• Multiple conference views in the same conference supporting dynamic layouts, auto-switching, and voice-activated video switching (requires EMP support).
	
	• Dynamic Layout mode switches the video image layout to match the number of participants in the conference as participants join and leave the conference (requires EMP support).
	
	• Auto-switching mode that periodically replaces participant images with those of other participants.
	
	• Flexible viewing options in cascaded conferences so you can view and manage cascaded participants.

Table 1-3   *Cisco IPVC 35xx MCU Feature Summary*

Feature	Description
Multi-view (dual-video)	The Cisco IPVC 35xx MCU supports dual-screen video and data transmissions to endpoints supporting two monitors using the H.239 standard or Tandberg DuoVideo. One monitor receives the conference video image and the other screen displays a presentation.
Rate matching features	The Cisco IPVC 35xx MCU offers a range of solutions for accommodating participants supporting different bandwidth rates in the same conference using the media processing capabilities of the Rate Matching Module (RMM) and Enhanced Media Processor (EMP) video processors.
	Each method for supporting variable bandwidth capabilities in a conference can be deployed by Cisco IPVC 35xx MCUs supported by the RMM. The EMP enables the Cisco IPVC 35xx MCU to support all these methods simultaneously in the same conference.
	The Cisco IPVC 35xx MCU supports the following rate matching features:
	• Symmetric Multi-layout Video—The Cisco IPVC 35xx MCU merges incoming data into a composite CP layout and sends it out at a rate equal to the incoming rate for the conference.
	• Mixed Rate—Video schemes (which include coding, bandwidth, and frame rates) are set for each conference, enabling the Cisco IPVC 35xx MCU to send video at optimum rates to different participants. With EMP support, you can configure up to three output schemes for each conference.
	• Dynamic—Maximum and minimum rates are pre-configured for each conference scheme setting. The Cisco IPVC 35xx MCU continuously adapts the bandwidth throughout the conference to the video conferencing terminal with the lowest bandwidth capacity.
Bandwidth optimization	The Cisco IPVC 35xx MCU supports the NetSave feature, which saves network resources by commanding participating endpoints to stop sending video streams when participants do not currently appear in the conference image.

Table 1-3   *Cisco IPVC 35xx MCU Feature Summary*

Feature	Description
Call handling capabilities	The Cisco IPVC 35xx MCU supports video conferencing up to 2.0 Mbps.
Port capacities	The Cisco IPVC 35xx MCU supports 100, 60, 30, or 15 ports depending on the Cisco IPVC 35xx MCU and license agreement. For example, the following port capacities are available on a Cisco IPVC 35xx MCU providing 100 ports: • Up to 150 calls at 64 Kbps (voice-only) • Up to 100 calls at 128 Kbps • Up to 70 calls at 384 Kbps • Up to 48 calls at 768 Kbps • Up to 26 calls at 1.5 Mbps • Up to 22 calls at 2.0 Mbps
Security and privacy	Password protection for a conference ensures privacy. Each unit is also protected by a password that an administrator can configure. The Cisco IPVC 35xx MCU features: • Administrator and operator password protection for accessing the Cisco IPVC 35xx MCU web interfaces. • Optional password protection for joining a conference and web access. Additional password protection for conference Chair Control.

Table 1-3   Cisco IPVC 35xx MCU Feature Summary

Feature	Description

H.235 Encryption for H.323 Calls	The Cisco IPVC 35xx MCU supports encrypted calls over IP networks. The encryption conforms to the H.325 standard and supports the following encryption algorithms:
	
	• DES: with an encryption key of 56 bits
	
	• AES: with an encryption key of 128 bits
	
	Encryption on the Cisco IPVC 35xx MCU can operate in one of the following modes:
	
	• Disabled—No encryption. The supported capability for this mode is Priority 1: no encryption.
	
	• Best effort—This mode implements a "best effort" encryption algorithm. If an endpoint supports encryption, it connects in an encrypted way. If not, it connects without encryption. The supported capabilities for this mode are:
	
	   – Priority 1: AES 128
	   – Priority 2: DES 56
	   – Priority 3: No encryption
	
	• Encryption required—This mode only connects encrypted calls. Encryption is either AES 128 or DES 56. Non-encrypted calls are not allowed to connect. The supported capabilities for this mode are:
	
	   – Priority 1: AES 128
	   – Priority 2: DES 56
	
	• Strong encryption required—This mode only allows AES 128 encrypted calls. Endpoints that do not support AES 128 are not allowed to connect. The supported capability for this mode is Priority 1: AES 128.
	
	The following channels support encryption:
	
	• Audio channel
	
	• Video channel
	
	• Far End Camera Control (FECC)
	
	Note All channels (audio, video, FECC, incoming, and outgoing) on the same call must have the same encryption levels. If the encryption on all channels cannot be achieved, the call disconnects.

Table 1-3   Cisco IPVC 35xx MCU Feature Summary

Feature	Description
IVR messages	The Cisco IPVC 35xx MCU includes pre-recorded greetings to conference participants and announcements as each new participant joins the conference. Using the Cisco IPVC Message Recording Utility, Interactive Voice Response (IVR) messages can be recorded to provide custom greetings and announcements. For further information on the Cisco IPVC Message Recording Utility, see the *User's Guide for Cisco IPVC 3525 Gateway* Release 2.0.

About the Cisco IPVC 3511 MCU

This section shows the front panel of the Cisco IPVC 3511 MCU and describes the connectors and LEDs.

Figure 1-1 and Table 1-4 show and explain the front panel of the Cisco IPVC 3511 MCU.

Figure 1-1   Cisco IPVC 3511 MCU
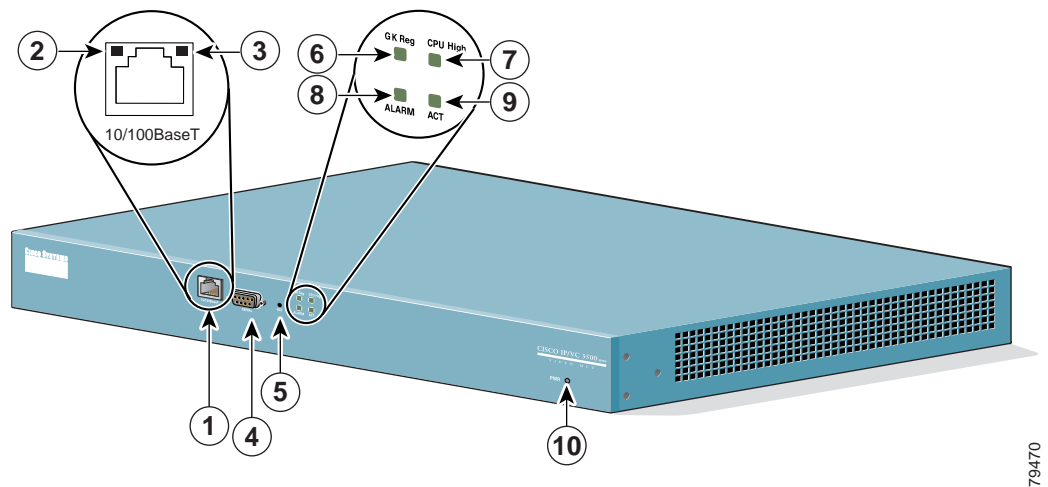
Table 1-4   Cisco IPVC 3511 MCU Figure Description

Number	Component	Description
1	10/100BaseT Ethernet port	A full-duplex Ethernet port that connects to the network through a standard RJ-45 connector.
2	Link LED	Lights when there is network activity.
3	Connectivity LED	Indicates the type of Ethernet interface in use. Lights green when the Ethernet interface is 100BaseT; off when the Ethernet interface is 10BaseT.

Table 1-4   Cisco IPVC 3511 MCU Figure Description

Number	Component	Description
4	Serial Port	An EIA-TIA-232 port that accepts a female DB-9 connector.
5	RST (Reset) Button	Restarts the Cisco IPVC 35xx MCU device.
6	GK Reg LED	Lights green when the Cisco IPVC 35xx MCU has an active registration with the gatekeeper.
7	CPU Hig LED	Lights green when 50% or more of the device processing capacity is in use.
8	Alarm LED	Lights orange when the Cisco IPVC 35xx MCU fails the self test during boot sequence or when there is a loss of frame alignment.
9	ACT LED	Lights green when there is call activity.
10	Power LED	Lights green when power to device is on.

About the Cisco IPVC 3511 MCU and EMP

This section shows the front panel of the The Cisco IPVC 3511 MCU and EMP and describes the connectors and LEDs.

Figure 1-2 and Table 1-5 show and explain the front panel of the Cisco IPVC 3511 MCU and EMP.

Figure 1-2   Cisco IPVC 3511 MCU and EMP
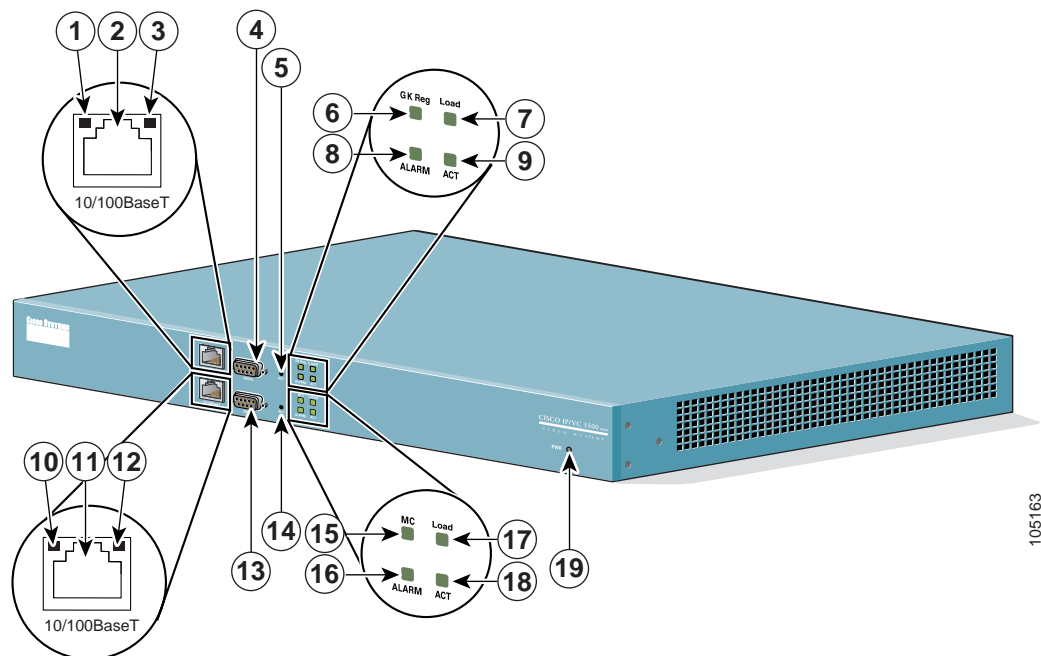
Table 1-5   Cisco IPVC 3511 MCU MCU and EMP Figure Description

Number	Component	Description
1	Link LED	Lights when there is network activity on the Cisco IPVC 35xx MCU.
2	10/100BaseT Ethernet port	A full-duplex Ethernet port for the Cisco IPVC 35xx MCU that connects to the network through a standard RJ-45 connector.
3	Connectivity LED	Indicates the type of Ethernet interface in use with the Cisco IPVC 35xx MCU. Lights green when the Ethernet interface is 100BaseT; off when the Ethernet interface is 10BaseT.
4	Serial Port	An EIA-TIA-232 port that accepts a female DB-9 connector for the Cisco IPVC 35xx MCU.
5	RST (Reset) Button	Restarts the Cisco IPVC 35xx MCU device.
6	GK Reg LED	Lights green when the Cisco IPVC 35xx MCU has an active registration with the gatekeeper.
7	CPU High	Lights green when 50% or more of the Cisco IPVC 35xx MCU processing capacity is in use.
8	Alarm LED	Lights orange when the Cisco IPVC 35xx MCU fails the self test during boot sequence or when there is a loss of frame alignment.
9	ACT LED	Lights green when there is Cisco IPVC 35xx MCU call activity.
10	Link LED	Lights when there is network activity on the EMP.
11	10/100BaseT Ethernet port	A full-duplex Ethernet port for the EMP that connects to the network through a standard RJ-45 connector.
12	Connectivity LED	Indicates the type of Ethernet interface in use on the EMP. Lights green when the Ethernet interface is 100BaseT; off when the Ethernet interface is 10BaseT.
13	Serial Port	An EIA-TIA-232 port that accepts a female DB-9 connector for the EMP.
14	RST (Reset) Button	Restarts the EMP device.
15	MC	Lights green when the EMP has an active registration with the Cisco IPVC 35xx MCU.
16	CPU High	Lights green when 50% or more of the EMP processing capacity is in use.
17	Alarm LED	Lights orange when the EMP fails the self test during boot sequence or when there is a loss of frame alignment.
18	ACT LED	Lights green when there is EMP call activity.
19	Power LED	Lights green when power to chassis is on.

About the Cisco IPVC 3540 MCU Module

The Cisco IPVC 3540 MCU is a module that installs in a Cisco IPVC 3544 chassis. The module has a 10/100BaseT Ethernet port on the front panel that uses an RJ-45 connector to connect to the network. There is an asynchronous, 9-pin serial-port that you can use with a hyperterminal program to configure and monitor the module.

The module has cPCI bus control circuitry that is used when it is installed in the top slot of the Cisco IPVC 3544 chassis. The module supports hot swapping when it is installed in chassis slots two, three, and four.

⚠
Caution   The module does not support "hot swapping" in the top slot where it can damage the board or the chassis or both.

There are three Cisco IPVC 3540 MCU module models. The models are distinguished by the number of user ports the module can simultaneously support at 128 Kbps. This value is referenced in the model number. The Cisco IPVC 3540 MCU modules can support 30, 60 or 100 user ports.

All modules provide cPCI bus control logic and can be installed in the chassis slot that controls the cPCI bus. A model number is silk-screened on the front panel of each module.

The model numbers are as follows:

- IPVC-3540-MC03A—Supports 30 user ports
- IPVC-3540-MC06A—Supports 60 user ports
- IPVC-3540-MC10A—Supports 100 user ports

Figure 1-3 and Table 1-6 show and explain a Cisco IPVC 3540 MCU module.

Figure 1-3   *Cisco IPVC 3540 MCU Module*
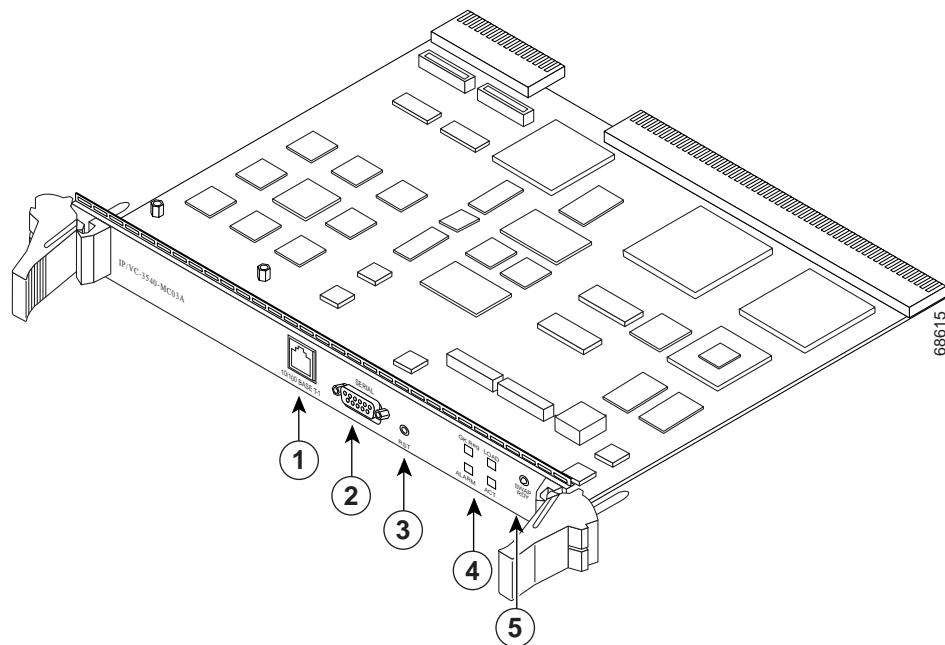
Table 1-6   Cisco IPVC 3540 MCU Module Figure Description

Number	Component	Description
1	10/100BaseT Ethernet port	This is a full-duplex Ethernet port that connects to the network through a standard RJ-45 connector.
2	Serial port	This is an EIA-TIA-232 port that accepts a male DB-9 connector. You can use the serial port to set the IP address for the module and to monitor Cisco IPVC 3540 MCU activity.
3	RST Button	This button resets the module. When the module is in the top chassis slot, this button resets the cPCI bus, and any other modules connected to the bus as well.
4	LEDs	• GK Reg—This LED is on when the Cisco IPVC 3540 MCU has an active registration with the gatekeeper. • Load—The load LED lights green when Cisco IPVC 3540 MCU processor at more than 50% of capacity. • Alarm—This LED indicates an error has occurred and the Cisco IPVC 3540 MCU requires resetting. • ACT—The Activity LED indicates there is call activity.
5	SWAP RDY	This LED lights blue when a Cisco IPVC 3540 MCU module in chassis slots 2, 3, or 4 is making contact with the connector in the chassis and the latches are open while the power is applied to the chassis. It is then safe to close the latches to secure the module or to remove the module from the chassis. You can hot swap modules in chassis slots 2, 3, and 4 only.

About Cisco IPVC 35xx MCU Networking Configurations

The Cisco IPVC 35xx MCU operates in different network configurations in conjunction with other network devices to provide video conferencing services.

About the Cisco IPVC 35xx MCU Architecture

The Cisco IPVC 35xx MCU enables both voice-only and multimedia conference calls for H.323, SIP, SCCP, H.320, and regular PSTN network telephones. Devices using the H.323 and SIP protocols can connect to a conference directly through the Cisco IPVC 35xx MCU. Other devices such as PSTN telephones and H.320 video conferencing terminals can connect to a conference through a gateway, such as the Cisco IPVC Gateway series.

The Cisco IPVC 35xx MCU supports devices that can send and receive video streams, as well as those that only receive video streams. This means that terminals without a video camera or video capturing capabilities can participate in a conference as voice-only participants while benefiting from seeing the other participants.

Figure 1-4 illustrates the devices and protocols that the Cisco IPVC 35xx MCU supports.

Figure 1-4   Supported Devices and Protocols
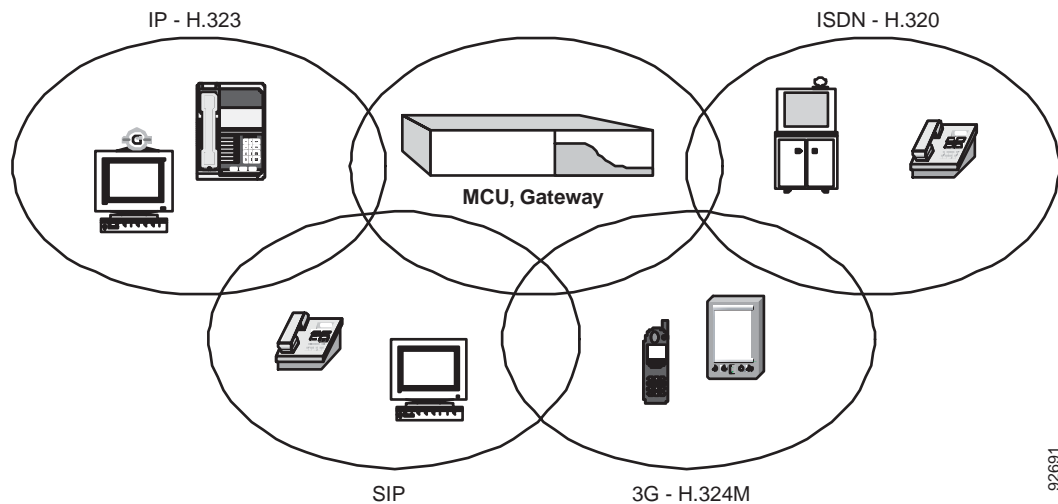
About Cisco IPVC 35xx MCU Components

The Cisco IPVC 35xx MCU comprises the following two basic components:

- Multipoint Controller (MC): The signalling component that manges call setup and conference control.
- Media Processor unit (MP): Processes the media content of the conference and performs functions such as audio mixing, video processing, data sharing, and switching. The MP works with the Real-time Transport Protocol (RTP) stream and is protocol independent.

The following devices operate as MP components under the management of the Cisco IPVC 35xx MCU:

- Cisco IPVC 35xx MCU operating in an MP Only mode.
- Enhanced Media Processor (EMP)
- Rate Matching Module (RMM)
- Cisco IPVC 3540 Application Server (AS) Module for Data Collaboration Server (DCS)

You can setup the MC and MP components of the Cisco IPVC 35xx MCU in the following physical configurations:

- Single Cisco IPVC 35xx MCU Board. See the "About the Single Cisco IPVC 35xx MCU Board Configuration" section on page 1-18 for more information.
- Cisco IPVC 35xx MCU with RMM. See the "About the Cisco IPVC 35xx MCU with RMM Configuration" section on page 1-18 for more information.
- Cisco IPVC 35xx MCU with EMP. See the "About the Cisco IPVC 35xx MCU with EMP Configuration" section on page 1-18 for more information.

About the Single Cisco IPVC 35xx MCU Board Configuration

In this configuration, the MC and MP components are both enabled and provide conference call setup and media processing supporting a voice-activated or a Continuous Presence (CP) layout of four images. This configuration has improved MC processing capabilities and an enhanced web management interface for improved Administrator monitoring, configuration, and conference control.

You can also configure the Cisco IPVC 35xx MCU to operate in an MP Only mode where the MC component is disabled and the Cisco IPVC 35xx MCU operates as a media processing module managed by a controlling the Cisco IPVC 35xx MCU in a clustering implementation.

About the Cisco IPVC 35xx MCU with RMM Configuration

In this configuration, the Rate Matching Module (RMM) supports the Cisco IPVC 35xx MCU to provide enhanced video processing capabilities including rate matching and increased range Continuous Presence (CP) layout combinations that allow the display of up to 16 participants for each conference.

About the Cisco IPVC 35xx MCU with EMP Configuration

In this configuration, the MC and audio media processing (MP) components are located on the Cisco IPVC 35xx MCU. The video MP is located on a separate EMP module. MC processing power is greatly increased for call setup, conference control, and audio processing. The EMP component of the Cisco IPVC 35xx MCU manages video processing capabilities and supports and extensive range of video layouts. This configuration supports up to three different layouts in the same conference on an EMP board, enabling you to support participants with different media processing capabilities.

About Cisco IPVC 35xx MCU Topologies

The MC and MP components of the Cisco IPVC 35xx MCU can work together or independently allowing the Cisco IPVC 35xx MCU to operate in a number of topologies to suit various network plans, accommodate different resource capabilities and expand the types of conferences possible. These topologies include:

- Centralized. See the "About the Centralized Topology" section on page 1-18 for more information.
- Clustered. See the "About the Clustered Topology" section on page 1-19 for more information.
- Cascaded Conferences. See the "About Cascaded Conferences" section on page 1-20 for more information.

About the Centralized Topology

In a centralized topology, the MC and MP components of the Cisco IPVC 35xx MCU work together to manage the conference signaling and to perform media processing for all connected terminals. The Cisco IPVC 35xx MCU can handle multiple conferences simultaneously. Figure 1-5 displays a centralized topology.

Figure 1-5   *Centralized Topology*
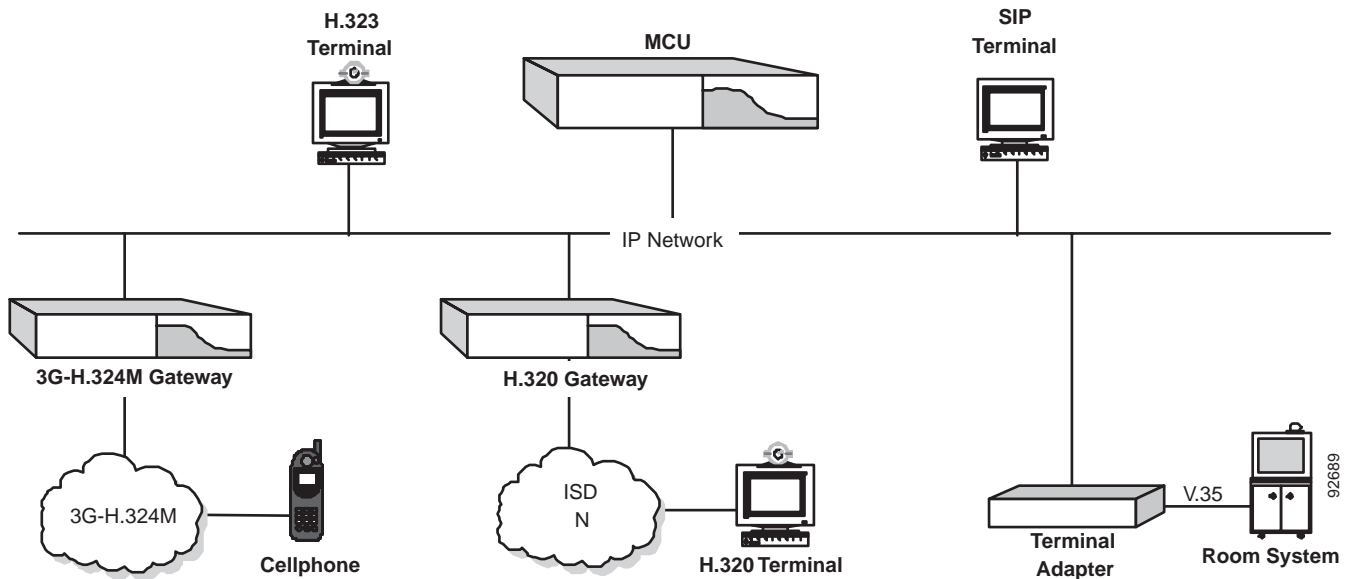
About the Clustered Topology

Since the MC and MP components of the Cisco IPVC 35xx MCU operate independently, the Cisco IPVC 35xx MCU can be set up in a clustered layout using a single MC that controls up to eight MP Only units. The MC component is disabled on Cisco IPVC 35xx MCU units configured as MP-only. The controlling Cisco IPVC 35xx MCU unit can make use of the on-board MP component as well. Additional MPs include the EMP and DCS.

The result of using a multi-MP layout is a significant increase in the number of concurrent audio, video, and data conferences you can run, as well as the number of total available calls that are possible utilizing a single controlling unit. Each MP unit can act as a media processor for a number of individual conferences.

Figure 1-6 demonstrates a typical scenario with four Cisco IPVC 35xx MCU units, each supporting multiple conferences with many participants, while one Cisco IPVC 35xx MCU unit performs all control and management functions.

Figure 1-6   Clustered Topology
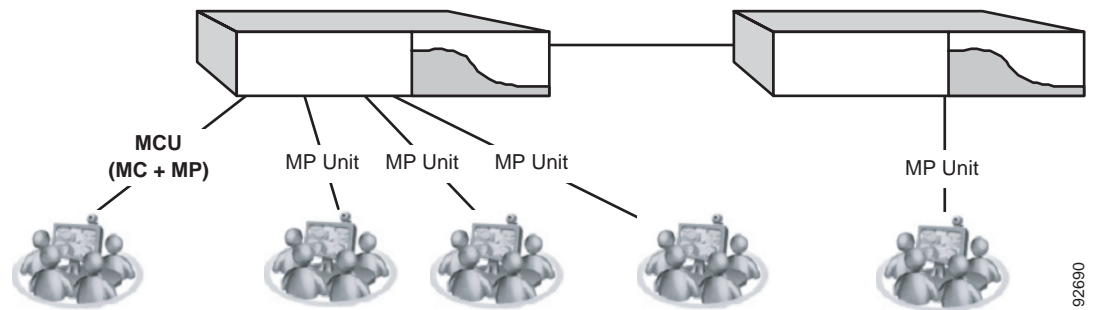
About Cascaded Conferences

With the Cisco IPVC 35xx MCU, you can combine two or more conferences resulting in a larger conference with many more participants. This is called cascading. Cascading creates a distributed environment that helps reduce the drain on network resources. In addition, the processing resources that the Cisco IPVC 35xx MCU requires are distributed between participating Cisco IPVC 35xx MCUs. Costly telephone or ISDN line usage can be further reduced with the mediation of a gateway.

Cascading occurs when one conference with "x" number of participants invites another conference with "y" number of participants. The two conferences effectively become one large conference. The bandwidth required across a cascaded conference link involving more than one Cisco IPVC 35xx MCU is only that of one audio/video stream between the two conferences. Each cascaded conference consumes significantly less than the accumulated bandwidth of all the participants. Each separate Cisco IPVC 35xx MCU unit participating in a conference retains control of its individual conference resources and participants.

Figure 1-7 demonstrates a typical conference over the IP network with one Cisco IPVC 35xx MCU. Four media streams are required, using four times the bandwidth. In Figure 1-8, the cascaded conference minimizes the use of network bandwidth by distributing processes amongst the participating Cisco IPVC 35xx MCUs.

Figure 1-7   Typical conference over the IP network with one Cisco IPVC 35xx MCU
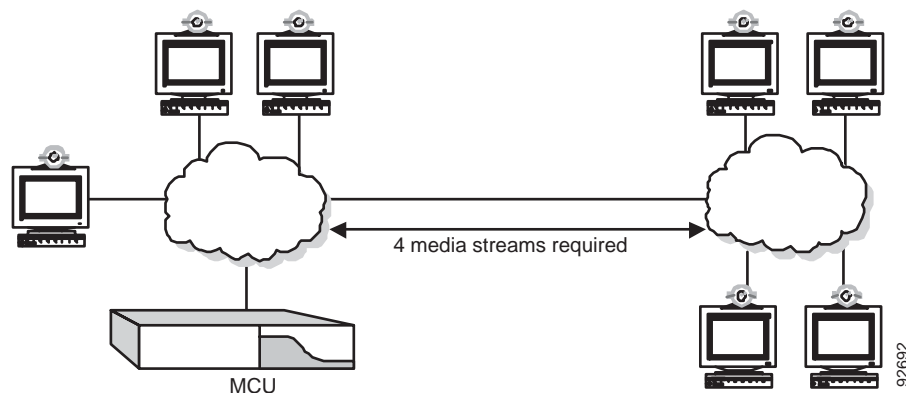
Figure 1-8   *Cascaded Conference*

Only 1 media stream required

MCU   MCU

92688
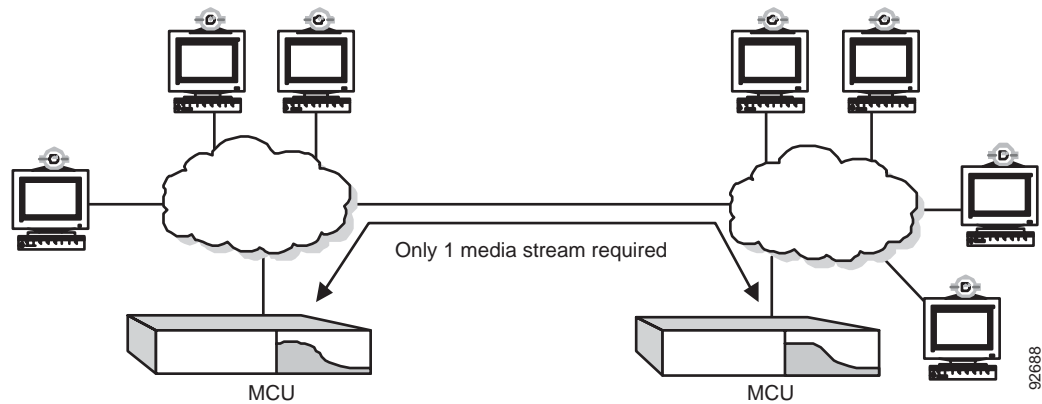
About Cisco IPVC 35xx MCU Multiple Protocol Support

The Cisco IPVC 35xx MCU supports calls from H.323, SCCP, and SIP endpoints in the same conference. The Cisco IPVC 35xx MCU supports H.320 and H.324 when operating with a gateway.

2

Installing the Cisco IPVC 35xx MCU

Revised: January 2006, OL-7777-03

This chapter describes the following topics:

Preparing for Installation

Warning During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.

This section describes the site requirements for installing a Cisco IPVC 35xx MCU. The requirements are as follows:

- Cisco IPVC 3544 chassis for Cisco IPVC 3540 MCU module

- PC with a serial port and terminal emulation software to assign the Cisco IPVC 35xx MCU an IP address

- Dedicated IP address for the Cisco IPVC 35xx MCU

- IP address of the router the Cisco IPVC 35xx MCU will use to communicate across the network

- For an H.323 environment, IP address of the H.323 gatekeeper with which you want the Cisco IPVC 35xx MCU to register

- For a Skinny Client Control Protocol (SCCP) environment, the IP address of the Trivial File Transfer Protocol (TFTP) server or Cisco CallManager from which you want the Cisco IPVC 35xx MCU to get configuration information

- 10BaseT or 100BaseT Ethernet cable

- Ambient room temperature range of 32° to 104°F (0° to 40°C) with a non-condensing relative humidity range of 15 to 85 percent

Verifying the Package Contents

Inspect the content of the box for shipping damage. Report any damage or missing items to your distributor or reseller. Table 2-1 lists the package content for the Cisco IPVC 3511 MCU and Cisco IPVC 3540 MCU module.

Table 2-1   Cisco IPVC 35xx MCUPackage Contents

Product	Contents
Cisco IPVC 3511 MCU	Cisco IPVC 3511 MCU packages contain the following items: • The Cisco IPVC 3511 MCU • Serial cable • Mounting rack kit (two brackets and three screws) • Four rubber feet • *Guide to Cisco Conferencing Documentation* • Regulatory Compliance and Safety Information for Cisco IPVC 3500 Products • Cisco IPVC Software CD-ROM • Cisco Information Package
Cisco IPVC 3540 MCU module	Your Cisco IPVC 3540 MCU module package contains the following: • Cisco IPVC 3540 MCU module • Terminal cable • *Guide to Cisco Conferencing Documentation* • Regulatory Compliance and Safety Information for Cisco IPVC 3500 Products • Cisco IPVC Software CD-ROM • Cisco Information Package

Mounting a Cisco IPVC 3511 MCU in a 19-inch Rack

This section describes how to install the brackets for mounting the unit on a 19-inch rack. You can install the Cisco IPVC 3511 MCU in a 19-inch rack or stack the unit with other Cisco IPVC 3511 MCU products up to four deep. The mounting kit supplied with the Cisco IPVC 3511 MCU includes two brackets for mounting the unit on a rack.

Warning **The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.**

Warning **Before opening the unit, disconnect the telephone-network cables to avoid contact with telephone-network voltages.**

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.**

Procedure

Step 1   Place the Cisco IPVC 3511 MCU right-side up on a hard flat surface, with the front panel facing you.

Step 2   Position a mounting bracket over the mounting holes on one side of the Cisco IPVC 3511 MCU, as shown in Figure 2-1.

Figure 2-1   *Fitting a Bracket for Rack Mounting*
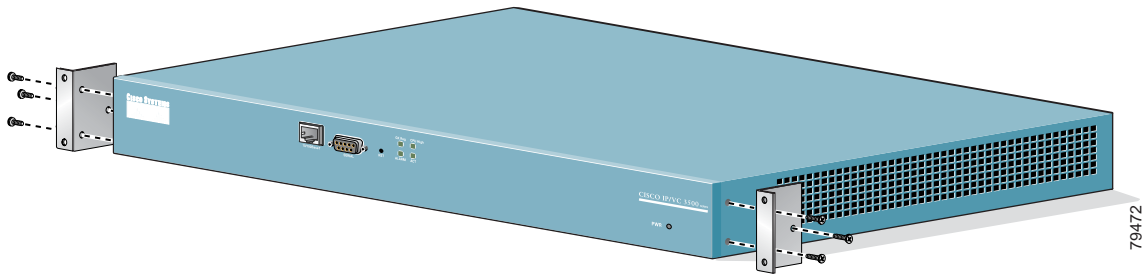
Step 3   Pass the three screws through the bracket holes, inserting them into the chassis and tighten them securely with a suitable screwdriver.

Step 4   Repeat Steps 2 and 3 for the other side of the Cisco IPVC 3511 MCU.

Step 5   Insert the unit into the 19-inch rack and secure with suitable screws.

Two screws are needed for each side. The Cisco IPVC 3511 MCU does not include them.

Step 6   Make sure that the air vents at the sides of the Cisco IPVC 3511 MCU are not blocked.

Installing a Cisco IPVC 3540 MCU Module in a Cisco IPVC 3544 Chassis

You must install a Cisco IPVC 3540 MCU module in a Cisco IPVC 3544 chassis. You can install the module in any slot in the chassis.

⚠

Warning   During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.

Procedure

Step 1   Do one of the following:

• When installing the module in the top slot of the chassis, make sure that the power to the chassis is off.

• To install the module in slots 2, 3, or 4, do the following:

– Loosen the screws that secure the latches of the top cover panel.

– Press the red buttons on each latch and snap the black handles back.

Step 2   Remove the Cisco IPVC 3540 MCU module from the antistatic bag.

Step 3   Insert the Cisco IPVC 3540 MCU module in the guide rails of the top slot and slide the module into the slot until the module connector makes contact with the chassis connector. (See Figure 2-2.)

Figure 2-2   Inserting the Cisco IPVC 3540 MCU Module
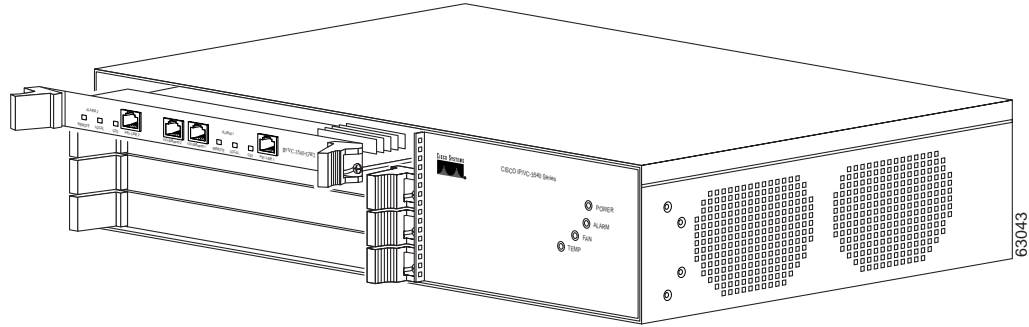
Step 4   Press the module firmly into the slot until the face plate is flush with the slot opening.

Warning   **Do not force the connectors. Forcing the connection can bend or damage the pins in the connector inside the chassis.**

Note   If you are installing the module in slots 2, 3, or 4, and the power to the chassis is on, the SWAP RDY LED on the module front panel lights blue when you slide the module into the chassis as far as it can go. This means that you can secure the module safely. The LED turns off when you close the handles.

Step 5   Snap the latch levers forward to secure the Cisco IPVC 3540 MCU module.

Step 6   If you install the module into the top chassis slot, plug the power cable into the chassis and turn on the power.

Warning   **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.**

Setting the IP Address

This section describes how to use the serial port to configure the unit with an IP address and other address information.

The serial port on the Cisco IPVC 35xx MCU front panel is used to assign a new Cisco IPVC 35xx MCU an IP address. You can assign the IP address before or after you connect the hardware to the network.

Before You Begin

Gather the items listed in Table 2-2 to assign an IP address to the Cisco IPVC 35xx MCU device.

Table 2-2   Requirements for Setting the IP Address

Requirements	Notes
Dedicated IP address for the Cisco IPVC 35xx MCU device	
IP address of the default router the Cisco IPVC 35xx MCU device uses to communicate over the network	
Subnet mask for the Cisco IPVC 35xx MCU device if applicable	
Domain Name Server and domain name for Cisco IPVC 35xx MCU if applicable	
PC with available serial port and terminal emulator software installed	
Null EIA/TIA-232 cable (shipped with the unit)	

Procedure

Step 1   Locate the serial cable shipped with the Cisco IPVC 35xx MCU and connect the end labeled PC to the serial port on the computer and the end labeled Unit to the serial port connector on the Cisco IPVC 35xx MCU front panel.

Step 2   Connect the power cable.

Step 3   Start the terminal emulator on the computer.

Step 4   Set the communication values for the terminal emulator as follows:

- 9600 Baud rate
- 8 data bits
- 1 stop bit
- No parity
- No flow control

Step 5   Turn on the power to the Cisco IPVC 35xx MCU.

A log of the auto-boot events appears on the computer.

Step 6   When the message "Press any key to start configuration" appears on the screen, press any key within six seconds.

The Main menu appears.

Step 7   At the prompt, enter **n** and press the **Enter** key to select the "Configure default network port" option.

Step 8   At the "Enter IP address for default interface" prompt, enter the IP address you want to assign to this Cisco IPVC 35xx MCU device and press **Enter**.

Step 9   At the "Enter Default Router IP Address" prompt, enter the IP address of the router that you want the Cisco IPVC 35xx MCU to use and press **Enter**.

Step 10   At the "Enter IP Mask <HEX> for default device" prompt, enter the subnet mask as follows:

- Convert the subnet mask IP address to hexadecimal notation, enter the hexadecimal number at the prompt, and press **Enter**.

    For example, for the subnet mask 255.255.255.0 the hexadecimal value you enter is FFFFFF00

> **Note**   You can use the computer's desktop calculator to convert the subnet mask ID to hexadecimal notation.

- If a subnet mask is not used, press **Enter**.

    After you enter the subnet mask parameter, the unit updates the boot line parameter and reboots.

Step 11   At the "Enter Preferred DNS Address for default Interface" prompt, enter the IP address of the primary DNS to which you want this Cisco IPVC 35xx MCU to register and press **Enter**.

Step 12   At the "Enter Alternate DNS Address for default Interface" prompt, enter the IP address of the secondary DNS to which you want this Cisco IPVC 35xx MCU to register and press **Enter**.

Step 13   At the "Enter DNS suffix for default Interface" prompt, enter the alias to which you want the DNS to associate this Cisco IPVC 35xx MCU and press **Enter**.

    Allow the unit to complete the reboot process. A new emulator session begins.

Step 14   At the Main menu, do one of the following:

- Enter the letter for the set of parameters that you want to configure.
- Enter **q** to save your changes and allow the device to complete the boot process.

Setting Ethernet Speed and Duplex Parameters

You can use the serial port to set the Ethernet speed and duplex parameters that you want the Cisco IPVC 35xx MCU to use.

> **Note**   We recommend that you manually set these parameters on the Cisco IPVC 35xx MCU and switch to Ethernet speed 100 Mbps and full duplex.

Procedure:

Step 1   Access the Cisco IPVC 35xx MCU through the serial port and start a terminal emulator session.

> **Note**   If the Cisco IPVC 35xx MCU is already running, you need to reboot or restart the device.

Step 2   When the message "Press any key to start configuration" appears on the screen, press any key within six seconds.

    The Main menu appears.

Step 3 At the prompt, enter **a** to select "Advanced configuration menu" and press **Enter**.

The Advanced configuration menu appears.

Step 4 At the prompt, enter **3** to select "Change LAN port Settings" and press **Enter**.

Step 5 At the prompt, enter the number or letter for one of the following:

- **1** - 10Mbps Half Duplex
- **2** - 100Mbps half Duplex
- **3** - 10Mbps Full Duplex
- **4** - 100Mbps Full Duplex
- **5** - Auto
- **Q** - Quit

  Enter this value to retain the current setting. The default setting is Auto.

Step 6 Press **Enter**.

The Main menu appears.

Step 7 At the Main menu, do one of the following:

- Enter the letter for the set of parameters that you want to configure.
- Enter **q** to save your changes and allow the device to complete the boot process.

Setting a TFTP Server

You can use the Cisco IPVC 35xx MCU as a video conference bridge for Cisco CallManager version 4.x and later. To set up the Cisco IPVC 35xx MCU to serve as a conference bridge, you must identify the TFTP server from which the Cisco IPVC 35xx MCU gets configuration information from the Cisco CallManager. You can enter that information using the serial port connection or the Administrator interface.

Procedure

Step 1 Access the Cisco IPVC 35xx MCU through the serial port and start a terminal emulator session.

> **Note** If the Cisco IPVC 35xx MCU is already running, you need to reboot or restart the device.

Step 2 When the message "Press any key to start configuration" appears on the screen, press any key within six seconds.

The Main menu appears.

Step 3 At the prompt, enter **t** and press the **Enter** key to select the "Configure TFTP server list" option.

Step 4 At the "TFTP Server # 0" prompt, enter the IP address of the first TFTP server you want the Cisco IPVC 35xx MCU to use and press **Enter**.

Step 5 At the "Would you like to add a new TFTP server [Y/N]" prompt, do one of the following:

- Press **y** and enter to identify another TFTP server that you want the Cisco IPVC 35xx MCU to use.

- Press **n** and enter to return to the main menu.

Step 6   At the Main menu, do one of the following:

- Enter the letter for the set of parameters that you want to configure.

- Enter **q** to save your changes and allow the device to complete the boot process.

This information appears in the SCCP Protocol Configuration dialog box in the Administrator interface. In this dialog box, you can configure the Cisco IPVC 35xx MCU to support Cisco CallManager as a SCCP conference bridge

Changing the Global User Name and Password

You can change the global user name and password that the Cisco IPVC 35xx MCU uses. You use this user name and password to access the configuration web page for the Cisco IPVC 35xx MCU, and is required for the following tasks:

- Starting a Telnet session to monitor the Cisco IPVC 35xx MCU

- Upgrading the Cisco IPVC 35xx MCU software

- Uploading Interactive Voice Response (IVR) messages to Cisco IPVC 35xx MCU configuration memory

The default global user name is admin. The default password is <null>.

Procedure

Step 1   Start a terminal emulator session as described in the "Setting the IP Address" section on page 2-7.

Step 2   At the prompt, enter **p**.

Step 3   At the "Enter User name" prompt, enter the name that you want to use for the global user name and press **Enter**.

Step 4   At the "Password" prompt, enter the password that you want to use and press **Enter**.

The Main menu appears.

Step 5   At the Main Menu, do one of the following:

- Enter the letter for the set of parameters that you want to configure.

- Enter **q** to save your changes and allow the device to complete the boot process.

Connecting the Cisco IPVC 35xx MCU to the LAN

This section describes how to connect the Cisco IPVC 35xx MCU to the Local Area Network (LAN).

Procedure

Step 1   Attach a cable from the network to the 10/100BaseT port on the Cisco IPVC 35xx MCU front.

Step 2   Turn on the power to the Cisco IPVC 35xx MCU.

Upgrading Cisco IPVC 35xx MCU Software

Software upgrades for the Cisco IPVC 3511 MCU and Cisco IPVC 3540 MCU module include the software components that are upgraded for the new version and a utility to upload the software to the unit. This section describes how to upgrade the software.

Procedure

Step 1   Download the upgrade software to a host that can access the Cisco IPVC 35xx MCU.

Step 2   Unzip the upgrade file.

Step 3   Double-click the upgrade.exe file.

The IPVC Upgrade utility appears.

Step 4   In the **Target IP** field, enter the IP address of the Cisco IPVC 35xx MCU for which you want to upload the software.

Step 5   In the **User Name** field, enter the software user name.

This is a global login name that the upload, upgrade, and telnet utilities use to log in to the Cisco IPVC 35xx MCU software. It can also be used to access the Administrator interface. The default user name is admin.

Step 6   In the **Password** field, enter the software password.

The default value is null.

> **Note**   To view the software components that will upgrade, click **Customize**. The Customize dialog box appears. If you do not want to upgrade a component, unselect it.

Step 7   Click **Upgrade**.

The upgrade process takes a few minutes. After the upload completes, the Upload Complete Message dialog box appears.

Step 8   Click **OK**.

Accessing the Cisco IPVC 35xx MCU Administrator Interface

In the Cisco IPVC 35xx MCU Administrator interface, you can configure general Cisco IPVC 35xx MCU settings, monitor Cisco IPVC 35xx MCU operation, create or edit services, manage MP units, and perform maintenance.

You access the Cisco IPVC 35xx MCU Administrator interface in the Cisco IPVC 35xx MCU access window by signing in as an Administrator.

Before You Begin

The following browser requirements are necessary to access the Cisco IPVC 35xx MCU Administrator interface:

- Microsoft Internet Explorer version 5.5 and later.

- The Cisco IPVC 35xx MCU IP address or a web link to the Cisco IPVC 35xx MCU.

Procedure

Step 1 Launch your browser and enter the IP address of the Cisco IPVC 35xx MCU.

The Cisco IPVC 35xx MCU access window appears.

Step 2 Click **Sign In**.

The access window displays the **Name** and **Password** fields.

Step 3 Enter the Administrator user name and password in the appropriate fields and click **Go**.

The Cisco IPVC 35xx MCU Administrator interface appears.

> **Note** If you try to sign in as an Administrator and another Administrator is currently signed in, the Cisco IPVC 35xx MCU signs you in as a **Read only** user and the words *Read Only* appear at the top of the window. **Read only** users cannot edit any of the Cisco IPVC 35xx MCU settings.

Using the Cisco IPVC 35xx MCU Setup Wizard

The Cisco IPVC 35xx MCU setup wizard runs automatically the first time you access the Cisco IPVC 35xx MCU Administrator interface. In the setup wizard, you can configure addressing for the Cisco IPVC 35xx MCU IP, H.323 gatekeeper, and Session Initiation Protocol (SIP) proxy. In the setup wizard, you can also set the regional date and time settings of the device on which you manage the Cisco IPVC 35xx MCU.

Procedure

Step 1 In the Administrator interface, click **MCU**.

Step 2 On the toolbar, click **Setup Wizard**.

> **Note** Note: The H.323 and SIP settings of the setup wizard appear where relevant according to the support for each protocol in your Cisco IPVC 35xx MCU license

The MCU Setup Wizard dialog box appears, displaying the Board Settings section.

Step 3 To change the IP address information with which the Cisco IPVC 35xx MCU is currently configured, follow these steps:

    a. In the **IP address** field, enter the IP address you want to assign to the Cisco IPVC 35xx MCU.

    b. In the **Subnet mask** field, enter the subnet mask you want to assign to the Cisco IPVC 35xx MCU.

    c. In the **Router IP address** field, enter the IP address of the router that you want the Cisco IPVC 35xx MCU to use.

    d. Click **Next**.

The H.323 Settings section appears.

Step 4 To set the gatekeeper you want the Cisco IPVC 35xx MCU to use, follow these steps:

    a. In the **Gatekeeper IP** field, enter the IP address of the gatekeeper that you want the Cisco IPVC 35xx MCU to use.

    b. In the **Gatekeeper Port** field, enter the port number that the Cisco IPVC 35xx MCU can use to communicate with the gatekeeper.

    c. Click **Next**.

The SIP Settings section appears.

Step 5 To change SIP configuration, follow these steps:

    a. In the **Proxy IP** field, enter the IP address for the SIP proxy.

    b. In the **Proxy Port** field, enter the port for the SIP proxy.

    c. In the **Default Domain** field, enter the default domain for the SIP proxy.

    d. Select the **Using Microsoft LCS** check box if the SIP proxy communicates with a Microsoft Live Communication Server device.

The Date and Time Settings section appears.

Step 6 To synchronize the Cisco IPVC 35xx MCU clock with the clock on the current computer, select the **Update to local time** check box.

Step 7 Click **Finish**.

Viewing General Information About the Cisco IPVC 35xx MCU

The Basics tab displays general information about the Cisco IPVC 35xx MCU. Table 2-3 describes the elements that appear in this tab.

Table 2-3   Board Basic Tab Elements

Field	Description
Board	Identifies the model number of the board or device.
Location	User-configured description about the device. Click this field to enter a new description, and then click **Upload** on the toolbar.
Serial number	The serial number that the factory assigned to the device.
Hardware version	The version number of the current hardware configuration
Date/Time	The date and time that the Cisco IPVC 35xx MCU clock reports.

Table 2-3   Board Basic Tab Elements

Field	Description
Slot number	Identifies the Cisco IPVC 3544 chassis slot in which this Cisco IPVC 3540 MCU module is inserted. For Cisco IPVC 3511 MCUs, slot 1 is the default slot.
Software version	Displays the version of software installed on the device. Click **Details** to view details on the versions of software components installed on the device.

Setting the Time and Date on the Cisco IPVC 35xx MCU

In the Basics tab, you can set the date and time that the Cisco IPVC 35xx MCU keeps.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **Board**.

Step 2   Make sure the **Basics** tab is selected.

Step 3   Next to the Date/Time field, click **Change**.

The Change Time dialog box appears.

Step 4   In the **Change** field, select the unit of time that you want to change:

- **Year**
- **Month**
- **Day**
- **Hour**
- **Minute**
- **Second**

> **Note**   There is no unit to change AM and PM. This designation rolls automatically when the hour rolls past 12 backward or forward. Similarly, seconds roll minutes, minutes roll hours, hours roll days, and days roll months.

Step 5   In the **Set board time to** field, choose the up or down arrow to change that unit.

The unit you choose changes in the direction you choose: higher (up) or lower (down).

Step 6   Repeat step 4-5 for as many units as you want to change.

Step 7   On the toolbar, click **Upload**.

Viewing Address Settings

In the Addressing tab, you can view address information for the Cisco IPVC 35xx MCU such as IP address informations, Domain Name Server (DNS) information, and Ethernet port speed and duplex.Table 2-4 describes the elements that appear on the Addressing tab.

Table 2-4   Addressing Tab Elements

Field	Description
IP Address	
IP Address	The IP address assigned to the Cisco IPVC 35xx MCU.
Router IP	The address of the router that Cisco IPVC 35xx MCU uses.
Subnet Mask	The subnet address that the Cisco IPVC 35xx MCU uses.
DNS	
DNS suffix	The DNS alias that the Cisco IPVC 35xx MCU uses.
Preferred DNS Server	The IP address of the primary DNS server that the Cisco IPVC 35xx MCU uses.
Alternate DNS server	The IP address of the alternative DNS server that the Cisco IPVC 35xx MCU uses.
Ethernet	
Port type	Displays information about the Ethernet connection.
Port settings	The Ethernet speed and duplex that the Cisco IPVC 35xx MCU uses.
MAC address	Displays the Mandatory Access Control (MAC) code assigned to the Cisco IPVC 35xx MCU device.
Port status	Displays the actual Ethernet speed and duplex the Cisco IPVC 35xx MCU uses on the network.

Related Topics

- Changing Address Settings, page 2-15

Changing Address Settings

In the Addressing tab, you can change the following address information for the Cisco IPVC 35xx MCU: IP address information, DNS information, and the Ethernet port speed and duplex.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **Board**.

Step 2   Click the **Addressing** tab.

Step 3   To change an IP address setting, do any of the following steps:

- In the **IP Address** field, enter the IP address you want to assign to the Cisco IPVC 35xx MCU.

- In the **Router IP** field, enter the IP address of the router you want the Cisco IPVC 35xx MCU to use.

- In the **Subnet Mask** field, enter the subnet mask you want the Cisco IPVC 35xx MCU to use.

Step 4   To change or add DNS information, do the following steps:

a.   In the **DNS suffix** field, enter the alias you want to assign to the current Cisco IPVC 35xx MCU.

b.   In the **Preferred DNS server** field, enter the IP address of the primary DNS server that you want the Cisco IPVC 35xx MCU to use.

c.   In the **Alternate DNS server** field, enter the IP address of the back-up DNS server that you want the Cisco IPVC 35xx MCU to use.

Step 5   In the **Port settings** field, choose the Ethernet port and duplex speed value you want to set.

Step 6   On the toolbar, click **Upload.**

Related Topics

-

About Administrators and Operators

Users must have authorization to access the Cisco IPVC 35xx MCU Administrator interface. You can also require users to have Operator-level access to perform management functions during conference calls.

Viewing Administrators and Operators

In the Users tabs, you can view user names that are registered with this Cisco IPVC 35xx MCU and their access level. Table 2-5 lists the elements that appear in Users tab.

Table 2-5   User Tab Elements

Field	Description
Name	The user login name
Access Level	The access privilege assigned to the user.
Telnet/FTP	Indicates whether the user is authorized to use Telnet or FTP to access the Cisco IPVC 35xx MCU.

Adding Administrators and Operators

In the Users tab, you can add Administrators.

Procedure

Step 1 In the Administrator interface, on the sidebar, click **Board**.

Step 2 Click the **Users** tab.

Step 3 Click the **Add**.

The Add User dialog box appears.

Step 4 In the **User name** field, enter the name you want the Administrator to log in with.

Step 5 In the **Access Level** field, choose the authorization level for this user:

- **Administrator**—Allows this user to launch the Administrator interface, use the Conference List that has links to web pages of current conferences, share conference chair control with another user, and access this device through Telnet, FTP, and the Cisco IPVC 35xx MCU Upgrade utility. You can assign up to ten users Administrator authorization.

- **Operator**—Allows this user to share conference chair control with another user and to access the Conference List that has links to web pages of current conferences. Up to 50 users can be assigned Operator authorization.

Step 6 In the **Password** field, enter the password this user uses to log in with.

Step 7 In the **Repeat Password** field, re-enter the password you entered in step 6.

Step 8 Select the **Enable for Telnet/FTP** check box to allow this user to access this device through Telnet and FTP.

Step 9 On the toolbar, click **Upload**.

Editing Administrator and Operator Settings

In the Users tab, you can edit the settings for a user with Administrator or Operator-level access.

Procedure

Step 1 In the Administrator interface, on the sidebar, click **Board**.

Step 2 Click the **Users** tab.

Step 3 Click the user you want to edit settings for.

Step 4 Click **Edit**

The Edit User dialog box appears.

Step 5 In the **User name** field, enter the name you want the Administrator to log in with.

Step 6 In the **Access Level** field, choose the authorization level for this user:

- **Administrator**—Allows this user to launch the Administrator interface, use the Conference List that has links to web pages of current conferences, share conference chair control with another user, and access this device through Telnet, FTP, and the Cisco IPVC 35xx MCU Upgrade utility. You can assign up to ten users Administrator authorization.

- **Operator**—Allows this user to share conference chair control with another user and to access the Conference List that has links to web pages of current conferences. Up to 50 users can be assigned Operator authorization.

Step 7   In the **Password** field, enter the password this user uses to log in with.

Step 8   In the **Repeat Password** field, re-enter the password you entered in step 6.

Step 9   Select the **Enable for Telnet/FTP** check box to allow this user to access this device through Telnet and FTP.

Step 10   On the toolbar, click **Upload**.

Deleting Administrators and Operators

You can delete users with Administrator or Operator-level access from the Cisco IPVC 35xx MCU system.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **Board**.

Step 2   Click the **Users** tab.

Step 3   Click the user you want to delete and then click **Delete**.

Configuring Security

You can configure the access that external programs have to the Cisco IPVC 35xx MCU. These external programs include Telnet, Simple Network Management Protocol (SNMP), File Transfer Protocol (FTP), and ICMP (Internet Control Message Protocol or "ping").

Procedure

Step 1   In the Administrator interface, on the sidebar, click **Board**.

Step 2   Click the **Security** tab.

Step 3   From the **Security mode** field, choose the access level you want the Cisco IPVC 35xx MCU to support:

- **Standard**—Allows SNMP, Telnet, FTP, and ICMP to access the Cisco IPVC 35xx MCU.

- **High (no Telnet or FTP)**—Allows access to the Cisco IPVC 35xx MCU only through SNMP and ICMP.

- **Maximum (no Telnet, FTP, SNMP, or ICMP)**—Disallows external programs to access the Cisco IPVC 35xx MCU.

Step 4   In the **SNMP Read community** and **Write community** fields, enter default strings used to enable SNMP communication between the Cisco IPVC 35xx MCU and a external application such as the MCU upload utility.

Step 5   Select the **Restrict access to this board according to the following rules** check box to set which IP ranges can access the Administrator interface. If you do not enable this setting, any IP address can access the Administrator interface. If you configure this setting, follow these additional steps:

    a.   In the **Allow access from these IP ranges** section, click **Add**.

       The Add IP Range dialog box appears.

    b.   In the **Please specify an IP range** fields, enter the starting and ending IP address of a range you want to allow.

    c.   Click **OK**.

    d.   In the **Block access from these IP ranges** section, click **Add**.

       The Add IP Range dialog box appears.

    e.   In the **Please specify an IP range** fields, enter the starting and ending IP address of a range you want to allow.

    f.   Repeat steps a-e as necessary to allow or block as many IP ranges as necessary.

    •   To edit an IP range, select it and click **Edit** in that section.

    •   To delete an IP range, select it and click **Delete** in that section.

Step 6   On the toolbar, click the **Upload**.

Registering the Online Help

The online help files for the Cisco IPVC 3511 MCU and Cisco IPVC 3540 MCU module Administrator and Conference Control interfaces are shipped on the Cisco IPVC Software CD-ROM. To use the online help, you must install the help files for the appropriate Cisco IPVC 35xx MCU in a shared directory on your network and register the directory location in the Administrator interface.

Procedure

Step 1   Open a Java-compliant web browser and enter the IP address of the Cisco IPVC 35xx MCU for which you want to make the online help available.

The Administrator login page appears.

Step 2   In the **Name** field, enter you user name.

Step 3   In the **Password** field, enter your password.

Step 4   Click **OK**.

Step 5   On the sidebar, click **Board**.

Step 6   Click the **Web** tab.

Step 7   In the **Online Help URL** field, enter the path to the directory in which the Cisco IPVC 35xx MCU online help files that you want to use are stored as follows:

    •   If the directory is located on a file server, enter:

file://.../shared_directory_name /program_folder

- If the directory is located on a web server, enter:

http://.../*shared_directory_name* /*program_folder*

Note   For Release 4.0, the online help files are stored in the folders mcu/4.0/admin/en/ by default. For Release 4.1, the online help files are stored in the folders mcu/4.1/admin/en/ by default. The Administrator interface searches in these files to retrieve online help text. In your path statement, include all directories in the path up to—but not including—the above mentioned help file path.

Step 8   On the toolbar, click **Upload**.

3

Configuring the Cisco IPVC 35xx MCU

Revised: January 2006, OL-7777-03

This chapter describes the following topics:

About the Administrator Interface

In the Administrator interface, you can configure Cisco IPVC 35xx MCU management policies, media processing, call management protocols, and services. Table 3-1 explains the tabs that appear in the Administrator interface.

Table 3-1 Administrator Interface Tabs

Tab Name	Description
Status	Enables you to view resource usage information and the number of calls and conferences currently in progress.
Settings	Enables you to define the Cisco IPVC 35xx MCU mode of operation.

Table 3-1   Administrator Interface Tabs

Tab Name	Description
Registered MPs	Enables you to view the MP units such as data and video processors and servers currently registered with the Cisco IPVC 35xx MCU and to edit MP settings.
MP Settings	Enables you to configure the local MP component and other MP units managed by the Cisco IPVC 35xx MCU.
Protocols	Enables you to set the gatekeeper IP address and the Session Initiation Protocol (SIP) registrar address for routing calls to the Cisco IPVC 35xx MCU from H.323, Skinny Client Control Protocol (SCCP), and Session Initiation Protocol (SIP) endpoints.
Services	Enables you to view, configure and edit the services that the Cisco IPVC 35xx MCU provides.
Event Log	Enables you to monitor Cisco IPVC 35xx MCU alarm events.

Figure 3-1 and Table 3-2 display and list the elements in the Administrator interface.

Figure 3-1   Administrator Interface
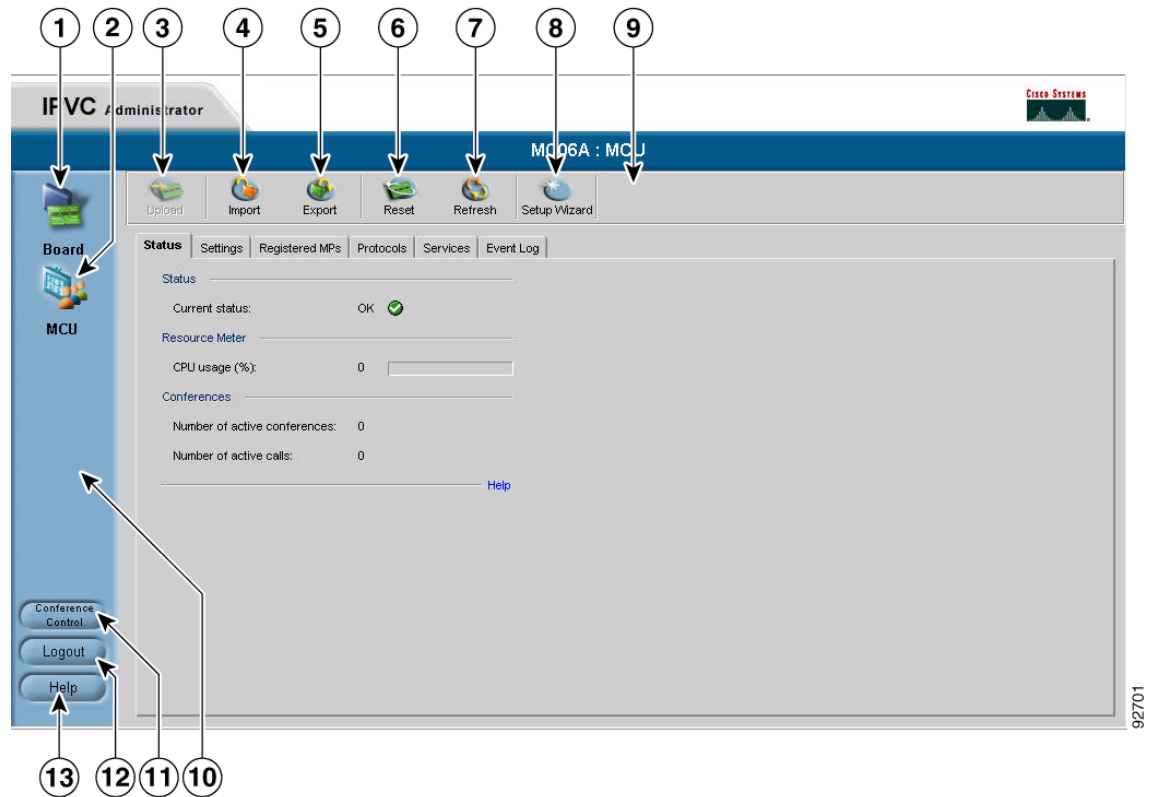
Table 3-2   Administrator Interface Elements

Number	Description
1	Board button
2	MCU button
3	Upload button
4	Import button
5	Export button
6	Reset button
7	Refresh button
8	Set Up Wizard button
9	Toolbar
10	Sidebar
11	Conference Control button
12	Logout button
13	Help button

Viewing the Status Tab

The Status tab displays information about Cisco IPVC 35xx MCU resource usage and performance. Table 3-3 lists the sections that appear in the Status tab.

Table 3-3   Status Tab Sections

Section Name	Description
Status	This section indicates the current operational status of the Cisco IPVC 35xx MCU as follows: • Error —Indicates that the Cisco IPVC 35xx MCU is not registered to a gatekeeper, or that the web XML connection (used for conference control) is down. • OK.
Resource Meter	This section contains the CPU Usage (%) field, which indicates the percentage of Cisco IPVC 35xx MCU resources currently occupied. We recommend that this value not exceed 90 percent.
Conferences	This section contains the following two fields: • Number of active conferences—Indicates the number of conferences currently hosted on the Cisco IPVC 35xx MCU. • Number of calls—Indicates the current number of calls on the Cisco IPVC 35xx MCU.

Configuring Cisco IPVC 35xx MCU Settings

In the Settings tab, you can perform the tasks described in the following sections:

- Configuring the Cisco IPVC 35xx MCU Operating Mode Basic Setting, page 3-5
- Setting the Cisco IPVC 35xx MCU Identifier Basic Setting, page 3-5
- Configuring SCCP Port Partition, page 3-5
- Configuring the Maximum Number of SCCP Conferences, page 3-6 (Release 4.1 only)
- Configuring Cisco IPVC 35xx MCU Conference Management Settings, page 3-6
- Configuring Cisco IPVC 35xx MCU Delimiters Settings, page 3-7
- Configuring DTMF Control, page 3-8
- Configuring Cisco IPVC 35xx MCU Themes, page 3-8
- Configuring Quality of Service for the Cisco IPVC 35xx MCU, page 3-9
- Configuring Cisco IPVC 35xx MCU Dynamic Layouts, page 3-11
- Configuring Cisco IPVC 35xx MCU Alert Indications, page 3-11
- Configuring Cisco IPVC 35xx MCU Advanced Settings, page 3-17
- Configuring Cisco IPVC 35xx MCU Themes, page 3-8

Configuring the Cisco IPVC 35xx MCU Operating Mode Basic Setting

In the Basics section of the Settings tab, you can select whether the Cisco IPVC 35xx MCU operates as a Multipoint Controller (MC) or only as a Media Processor (MP).

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Settings** tab.

Step 3   Click the **Basics** button (If not already selected).

Step 4   In the **MCU Mode** field, make one of the following choices:

- **MCU**: The Cisco IPVC 35xx MCU operates as an MC and MP unit. It can also manage up to six additional registered MP-only units in a multi-MP layout to support a proportionately higher number of participants. This is the default setting.

- **MP Only**: The MP component is enabled and the MC component disabled while operating under the control of another Cisco IPVC 35xx MCU. A Cisco IPVC 35xx MCU configured for MP-only mode processes conference media content and performs functions such as audio mixing, video processing, and switching.

Setting the Cisco IPVC 35xx MCU Identifier Basic Setting

In the Basics section of the Settings tab, you can set the Cisco IPVC 35xx MCU identifier. This identifies the Cisco IPVC 35xx MCU in the following situations:

- During gatekeeper registration and in call setup—The registration name sent to the gatekeeper/SIP registrar is a concatenation of the Cisco IPVC 35xx MCU identifier and IP address.

- Inviting endpoints—When inviting endpoints into a conference, the Cisco IPVC 35xx MCU identifier forms part of the alias for the Q.931 signaling, together with the conference identifier.

- Text overlay in cascaded conferences—The Cisco IPVC 35xx MCU identifier forms the text overlay for the cascaded Cisco IPVC 35xx MCU

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Settings** tab.

Step 3   Click the **Basics** button (If not already selected).

Step 4   In the **MCU Identifier** field, enter an identifier (up to a maximum of 15 characters).

Configuring SCCP Port Partition

In the Basics section of the Settings tab, you can configure the number of Cisco IPVC 35xx MCU ports partitioned for the Skinny Client Control Protocol (SCCP) rather than for the H.323 or SIP protocols.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Settings** tab.

Step 3   Click the **Basics** button (if not already selected).

Step 4   In the **Number of SCCP ports** field, choose the number of ports you want to partition for SCCP. Choosing **0** disables SCCP support.

Configuring the Maximum Number of SCCP Conferences

Note   This section applies only to Release 4.1.

In the Basics section of the Settings tab, you can set the number of reserved SCCP conferences. Reserving SCCP conferences preserves Enhanced Media Processor (EMP) resources for SIP/H.323 conferences.

If you choose not to configure this setting, the Cisco IPVC 35xx MCU uses the default setting. The default number of reserved SCCP conferences is the number of supported SCCP ports divided by three. The SCCP service bandwidth determines the number of SCCP ports.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Settings** tab.

Step 3   Click the **Basics** button (if not already selected).

Step 4   Select the **Set manually** check box.

Step 5   In the **Max SCCP conferences** field, enter the number of SCCP conferences you want to reserve.

Configuring Cisco IPVC 35xx MCU Conference Management Settings

In the Conference Mgmt section of the Settings tab, you can configure settings for conference registration with the gatekeeper and determine how participants can create and join conferences.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Settings** tab.

Step 3   Click the **Conference Mgt** button.

Step 4   Select the **Register conference ID** check box to register existing conference IDs with the gatekeeper and SIP server to enable participants dialing in to a conference from remote locations to connect to the target conference on the Cisco IPVC 35xx MCU. This setting is unselected by default.

> **Note**   If SIP is supported and you enable this option, you must configure a registrar.

Step 5   In the **External conference authorization policy** field, choose one of the following Cisco IPVC 35xx MCU authorization policies for creating or joining conferences:

- **None**—No authorization required.

- **Notify**—The Cisco IPVC 35xx MCU notifies an external application such as a conference scheduler that accesses or controls Cisco IPVC 35xx MCU resources about conference creation or joining.

- **Authorize**—The Cisco IPVC 35xx MCU requests authorization from an external application such as a conference scheduler which accesses or controls Cisco IPVC 35xx MCU resources to create conferences or allow participants to join conferences.

Step 6   In the **Allow conference creation using** field, choose one of the following methods through which conferences can be created:

- **Scheduler only**—Enables conference creation only using a conference scheduling application

- **Scheduler, Web and Control API**—Enables conference creation using a conference scheduling application, the Conference Control interface, or an external application that uses the Cisco IPVC 35xx MCU API.

- **Scheduler, Web, Control API and dial-in** (default)**—**Enable all the conference creation methods listed above, as well as dial-in for ad-hoc conference creation.

Step 7   Select the **When using the web, only operators or administrators can create a conference** check box to grant conference creation authorization only to users with Administrator or Operator privileges. If you want users with all levels of access to be able to create a conference, leave this option unselected.

Step 8   In the **Allow conference joining using** field, choose one of the following methods through which participants can join a conference:

- **Invite only**—Participants can join a conference only when the Cisco IPVC 35xx MCU dials that participant.

- **Invite and dial-in**—Participants can join a conference either by Cisco IPVC 35xx MCU invitation or by dialing directly using a conference ID.

Step 9   In the **Dial-in conference terminates when** field, choose the method through which dial-in (ad hoc) conferences terminate:

- **Last participant leaves**—The conference terminates when the last participant leaves the conference.

- **Conference creator leaves**—The conference terminates when the conference creator leaves the conference.

Configuring Cisco IPVC 35xx MCU Delimiters Settings

The Delimiters section of the Settings tab enables you to configure password and invitation delimiters.

Procedure

Step 1	In the Administrator interface, click the **MCU** button (If not already selected).
Step 2	Click the **Settings** tab.
Step 3	Click the **Delimiters** button.
Step 4	In the **Password delimiter** field, enter the characters used as a separator between the conference ID and conference password when dialing into a conference. A conference is created with this password if no conferences already exist with the specified number. Valid delimiters include the pound sign (#) and asterisk (*). The default password delimiter setting is three asterisks (***).
Step 5	In the **Invite delimiter** field, enter the characters used to separate participant numbers in multiple participant invitation. Valid delimiters include the pound sign (#) and asterisk (*). The default invite delimiter setting is two asterisks (**).

Configuring DTMF Control

In the DTMF Control section of the Settings tab, you can active Dual Tone Multi-Frequency (DTMF) conference control. With DTMF conference control, you can perform the following functions:

- Take or release Chair Control.
- Mute or unmute your line
- Control your volume
- Block or unblock admission to a conference (Chair Control users only)
- Invite new participants (Chair Control users only

Procedure

Step 1	In the Administrator interface, click the **MCU** button (If not already selected).
Step 2	Click the **Settings** tab.
Step 3	Click the **DTMF Control** button.
Step 4	Select the **Enable DTMF Conference control** check box to enable DTMF conference control.
Step 5	In the **DTMF Conference Control prefix** field, choose a symbol for starting the DTMF conference control session. You can select pound (#) or asterisk (*). The default is *.

Configuring Cisco IPVC 35xx MCU Themes

In the Themes section of the Settings tab, you can preview pre-configured video display settings and configure custom themes. You select theme options when configuring services. You can configure a custom theme specifying the text font, color, background color, and border settings for active participants.

Note   This feature requires Enhanced Media Processor (EMP) support.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Settings** tab.

Step 3   Click the **Themes** button.

Step 4   In the **Default theme** field, choose one of the following themes:

- **Basic**
- **Blue Freeze**
- **Copper Autumn**
- **Charlie Chaplin**
- **Fresh Green**

If you choose any theme other than Basic, the font, subframe, and border color are automatically set. If you select **Basic**, follow steps 5-8 below.

Step 5   In the **Font background transparency** field, choose one of the following settings:

- **None**—A solid background against which the text appears.
- **Half**—A moderate background against which the text appears.
- **Full**—A transparent background against which the text appears.

Step 6   In the **Font size** field, choose a font size:

- **Small**
- **Normal**
- **Large**

Step 7   In the **Font foreground color**, **Font background color**, **Empty subframe color**, **Default border color**, and **Active speaker border color** fields, click to select a color for these settings.

Step 8   The Basic font field displays the font currently installed on the Cisco IPVC 35xx MCU. Select the **Enable extended font** check box to enable an additional font if one is installed on the Cisco IPVC 35xx MCU.

You can view the effects of your settings in the Preview section. This section displays the selected theme settings. This includes: a layout with four sub-frames; the theme border highlight colors; active speaker border highlight color; font formatting; screen background color; and text background settings.

Configuring Quality of Service for the Cisco IPVC 35xx MCU

In the Quality of Service section of the Settings tab, you can assign a priority level to video and voice calls. This section describes how to configure these Quality of Service (QoS) settings using either pre-configured system settings or by creating your own settings.

Quality of Service settings involves configuring the Cisco IPVC 35xx MCU to add a Quality of Service (QoS) IP Precedence code in the IP header of outbound packets. Routers on the network that support QoS can give precedence to such coded packets and facilitate the efficient transmission of packets. You can set priority levels on the Cisco IPVC 35xx MCU for voice calls, video calls, or both.

The Type of Service (ToS) field in the IP header contains eight bits and indicates the following three abstract quality of service parameters:

- Delay (D)
- Throughput (T)
- Reliability (R)

You use the abstract parameters to choose the actual service parameters when transmitting a datagram through a particular network. The abstract parameters represent the three-way trade off between low delay, high throughput, and high reliability. Increasing the performance of one of these parameters might result in reduced performance of the other two. Figure 3-2 represents the ToS field in the IP header.

Figure 3-2   TOS Field in the IP Header
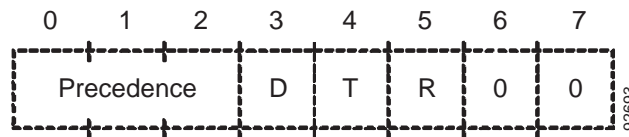
Note   The same fields can also be used to set DiffServ codepoint values

---

The function of each bit of the ToS field is as follows

- Bits 0-2: Precedence (an independent measure of the importance of the datagram)
- Bit 3: 0 = normal delay, 1 = low delay
- Bit 4: 0 = normal throughput, 1 = high throughput
- Bit 5: 0 = normal reliability, 1 = high reliability
- Bits 6-7: reserved for future use

The possible Precedence settings are as follows:

- 111 = Network Control
- 110 = Internetwork Control
- 101 = CRITIC/ECP
- 100 = Flash Override
- 011 = Flash
- 010 = Immediate
- 001 = Priority
- 000 = Routine

Procedure:

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Settings** tab.

Step 3   Click the **Quality of Service** button.

Step 4   In the **Quality of service support** field, set the required IP ToS value for each media type by clicking one of the following radio buttons:

- **None**—Select to disable Quality of Service support

- **Default**—Select to assign the default IP ToS value for each media type. The default settings represent Cisco recommendations.

- **Custom**—Select to assign your own IP ToS value for each media type.

If you select **Default**, the system automatically enters Quality of Service settings. If you select **Custom**, follow the steps below.

Step 5   In the **Voice Priority** field of the Video Calls section, enter a whole number from 0 to 63 to set the priority level of voice packets that the Cisco IPVC 35xx MCU sends out. The default value is 34.

Step 6   In the **Video Priority** field of the Video Calls section, enter a whole number from 0 to 63 to set the priority level of video packets that the Cisco IPVC 35xx MCU sends out. The default value is 34.

Step 7   In the **Voice Priority** field of the Voice Calls section, enter a whole number from 0 to 63 to set the priority level of voice packets that the Cisco IPVC 35xx MCU sends out. The default value is 46.

Configuring Cisco IPVC 35xx MCU Dynamic Layouts

In the Dynamic Layouts section of the Settings tab, you can define the exact layout transition order that conferences including different numbers of participants use.

Dynamic layouts are activated individually for each service. When selected, the conference layout changes automatically as participants join or leave.

Note   This feature requires EMP support.

Procedure

Step 1   In the Administrator interface, click **MCU** (if not already selected).

Step 2   Click the **Settings** tab.

Step 3   Click the **Dynamic Layouts** button.

Step 4   Click a layout image to select or deselect that specific layout.

Configuring Cisco IPVC 35xx MCU Alert Indications

In the Alert Indications section of the Settings tab, you can select which events trigger Simple Network Management Protocol (SNMP) traps. You can also define multiple SNMP servers to which the Cisco IPVC 35xx MCU sends the SNMP traps and configure which events to display in the Event Log tab.

About SNMP Trap Types

All Cisco IPVC 35xx MCU SNMP traps have the following structure:

```
rvGenNotification NOTIFICATION-TYPE
OBJECTS{
rvApplIndex,
rvTrapTimeStamp,
rvTrapEventType,
rvTrapSeverity,
rvTrapMessage,
        rvUnitType,
        rvTrapIndex,
        ipAdEntAddr
}
STATUScurrent
DESCRIPTION
"Defines general trap structure."
::= { rvGeneralNofications 1}Message}
```

The OID of the rvGenNotification trap is 1.3.6.1.4.1.903.8.0.1.

Note   The RV object identifier reference= 1.3.61.4.1.903.

About SNMP Trap Structure

Table 3-4 lists the Cisco IPVC 35xx MCU SNMP trap structure.

Table 3-4   *Cisco IPVC 35xx MCU SNMP Trap Structure*

Field	OID	Syntax	Description
rvApplIndex	RV.1.9.2.1.2	Integer	Indicates type of application: 1=Gateway 2=Cisco IPVC 35xx MCU 3=Cisco IOS Gatekeeper
rvTrapTimeStamp	RV.1.9.2.1.3	DateAndTime	Indicates the time at which the trap event occurred. Byte format: 1-2=year (0 to 65536.) 3=month (1 to 12). 4=day (1 to 31). 5=hour (0 to 23). 6=minutes (0 to 59). 7=seconds (0 to 60) **Note** Use 60 for leap-seconds. 8-deciseconds (0 to 9). 9=direction from UTC "+"/"-". 10=hours from UTC (0 to 13). 11=minutes from UTC (0 to 59).
rvTrapEventType	RV.1.9.2.1.4	RvEventType	Indicates the type of SNMP trap.
rvTrapSeverity	RV.1.9.2.1.5	Integer	Indicates the severity of the SNMP trap: 0=cleared 1=information 2=critical 3=major 4=minor 5=warning **Note** You configure trap severities in the Alert Indications section of the Settings tab. See the "Configuring SNMP Trap Servers" section on page 3-14 for more information.
rvTrapMessage	RV.1.9.2.1.6	String	A text message describing the nature of the problem is sent for each trap.
rvUnitType	RV.1.1.9	Integer	Represents the type of sending unit. The Cisco IPVC 35xx MCU sends the identifying number 196612.

Table 3-4   *Cisco IPVC 35xx MCU SNMP Trap Structure*

Field	OID	Syntax	Description
rvTrapIndex	RV.1.9.2.1.1	Integer	Represents the trap index in the trap log table.
ipAdEntAdd	1.3.6.1.2.1.4.20.11	IpAddress	Represents the IP address of the sending unit.

Configuring SNMP Trap Servers

In the Alert Indications section of the Settings tab, you can define the IP address, port, and enabled traps for SNMP trap servers.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Settings** tab.

Step 3   Click the **Alert Indications** button.

Step 4   In the SNMP Traps Server section, click **Add**.

The SNMP Trap Servers Properties dialog box appears.

Step 5   In the **SNMP Trap server address** field, enter the address for the SNMP trap server.

Step 6   In the **Port** field, enter the port of the SNMP trap server. The default port for SNMP servers is 162.

Step 7   In the Enabled traps section, select which traps you want to enable:

- To disable a trap, click it in the Enabled traps area and then click **Remove**.
- To enable a trap, click it in the Disabled traps area and then click **Add**.
- To enable all traps, click **Add All**.
- To disable all traps, click **Remove All**.

Step 8   Click **Upload** to save your settings.

The configured SNMP trap server appears in the SNMP Trap Servers section.

Editing Configured SNMP Trap Servers

In the Alert Indications section of the Settings tab, you can edit a configured SNMP trap server.

Step 1   In the Administrator interface, on the sidebar, click **MCU** (If not already selected).

Step 2   Click the **Settings** tab.

Step 3   Click the **Alert Indications** button.

Step 4   In the SNMP Trap Servers section, click the configured SNMP trap server and then click the **Edit** button.

Step 5   Click **Upload** when you finish your edits.

Deleting Configured SNMP Trap Servers

You can delete configured SNMP trap servers in the Alert Indications section of the Settings tab.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Settings** tab.

Step 3   Click the **Alert Indications** button.

Step 4   In the SNMP Trap Servers section, click the configured SNMP trap server and then click **Delete**.

Setting Cisco IPVC 35xx MCU Alert Indications

In the Alert Indications section of the Settings tab, you can configure alert indications in the Administrator interface.

Table 3-5 lists alert indications as well as the SNMP trap (as detailed in the RvEventType textual convention) associated with them.

Table 3-5   *Cisco IPVC 35xx MCU Alert Indications*

Event Type	Trap Name	rvTrapEvent Type Value	Trap is sent when...
Abnormal disconnect	abnormalDisconnect	11	A call disconnects for a reason other than normal, busy, or no answer.
Call disconnected by remote endpoint	remoteDisconnect	42	A call disconnects normally by a remote endpoint.
Card extract/Hot swap	cardExtractHotSwap	10	A card has been removed from the chassis under power or inserted into the Cisco IPVC 3544 chassis under power.
Cold start	coldStart	1001	The Cisco IPVC 35xx MCU has been activated by inserting the card into a Cisco IPVC 3544 chassis under power or has been reset using the button on the front panel of the board.
Corrupt WEB data	corruptWebData	15	Corrupt web files are present in the Cisco IPVC 35xx MCU.
Gatekeeper registration state change	gkRegistrChange	5	A change occurs in the registration status of the Cisco IPVC 35xx MCU with the gatekeeper.
General alarm	generalAlarm	31	A system failure is detected.

Table 3-5   Cisco IPVC 35xx MCU Alert Indications

Event Type	Trap Name	rvTrapEvent Type Value	Trap is sent when...
Incompatible software version install	incompatibleSwBurnAttemp	73	An attempt to burn a version of the Cisco IPVC 35xx MCU software onto incompatible hardware occurs.
Link down	linkDown	1003	Standard SNMP MIB trap indicating that the network connection is down with details about the cause and time of connection loss.
Link up	linkUp	1004	Standard SNMP MIB trap indicating that the network connection has been reestablished.
Loss of Ethernet	lossEthernet	7	The network returns after going down. Indicates the time at which the network was restored. The time is contained in the rvTrapMessage.
MP lost	mpLost	28	Communication with a registered MP has broken. This includes of a description of the MP contained in the rvTrapMessage.
Max resource meter	maxHighLevelResMeter	8	A high CPU level (85%) is reached in the Cisco IPVC 35xx MCU.
Network problem	networkProblem	9	A problem occurs on the network.
Overheating	overheating	30	The configured temperature thresholds for the device are exceeded. Overheating can cause serious damage to the functioning of the device.
Power-down	powerDown	4	The Cisco IPVC 35xx MCU is shutting down.
Power-up	powerUp	3	The Cisco IPVC 35xx MCU has begun operation.
Services table is changed	mcuServiceTableChanged	29	The service table has been modified.
Warm start	warmStart	1002	A Cisco IPVC 35xx MCU reset has been performed using the Administrator interface.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Settings** tab.

Step 3   Click the **Alert Indications** button.

Step 4   In the Events section, select the check boxes in the Enabled in the Event Log column for all the events that you want to trigger SNMP traps.

Step 5   For each event you enable, choose one of the following severities in the Severity column:

- **Cleared**—Enumeration 0. One or more previously reported alarms have been cleared.

- **Information**—Enumeration 1. Notification of a non-erroneous event.

- **Critical**—Enumeration 2. A service-affecting event has occurred and requires immediate corrective action.

- **Major**—Enumeration 3. A service-affecting event has occurred and requires corrective action to prevent the condition becoming more serious.

- **Minor**—Enumeration 4. A non-service-affecting event has occurred and requires corrective action to prevent the condition becoming more serious.

- **Warning**—Enumeration 5. A potential or impending service-affecting event has been detected, but no significant events have occurred yet. Action should be taken to further diagnose and correct the problems to prevent the condition becoming more serious.

Tips

You can click the **Select All** button to select all events or the **Clear All** button to clear all events.

Configuring Cisco IPVC 35xx MCU Advanced Settings

In the Advanced section of the Settings tab, you can perform the tasks described in the following sections:

- Setting the User Interface Language, page 3-17

- Setting an Operator Number, page 3-18

- Configuring Participant Name Display Duration, page 3-19

- Disconnecting Participants on Communications (ICMP) Failure, page 3-19

- Configuring the NetSave Feature, page 3-20

- Sending Advanced Commands, page 3-20

- Opening a Telnet Terminal, page 3-23

Setting the User Interface Language

In the Advanced section of the Settings tab, you can configure the language that the Cisco IPVC 35xx MCU supports. Table 3-6 lists the languages that the Cisco IPVC 35xx MCU supports.

Table 3-6   Supported Languages in the Cisco IPVC 35xx MCU User Interface

Language	Administrator Interface	Conference Control Interface	Text Overlay on Conference Video
English	*	*	*
Chinese	*	*	*
Japanese	*	*	*
Portuguese	*	*	*

Note To view Chinese or Japanese fonts properly in the Administrator interface, the computer (where the web browser is running) should support the appropriate languages. You should set its default language (which you select from the **Control Panel > Regional and Language Options** menu) accordingly.

Procedure

Step 1 In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2 Click the **Settings** tab.

Step 3 Click the **Advanced** button.

Step 4 In the **User Interface** language field, select one of the following languages:

- **English**
- **Chinese**
- **Japanese**
- **Portuguese**

Setting an Operator Number

During a conference, you can invite an Operator to join and provide consultation and support. To do this, in the Advanced section of the Settings tab, you set the number of the designated operator that the Cisco IPVC 35xx MCU dials when a user clicks the Operator button in the Conference Control interface.

Procedure

Step 1 In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2 Click the **Settings** tab.

Step 3 Click the **Advanced** button.

Step 4 In the **Operator** number field, enter an operator number.

Configuring Participant Name Display Duration

In the Advanced section of the Settings tab, you can configure the duration during which a participant name appears in a conference.

Before You Begin

This setting applies only to conferences for which the Display participant name setting is set to On change in the view settings of a service. See the "Editing View Settings" section on page 3-53 for more information.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Settings** tab.

Step 3   Click the **Advanced** button.

Step 4   In the **Participant name display duration (sec)** field, enter a duration in seconds.

Disconnecting Participants on Communications (ICMP) Failure

You can configure the Cisco IPVC 35xx MCU to disconnect a call when an endpoint becomes unreachable. When configured this way, the Cisco IPVC 35xx MCU identifies inactive Real-Time Transport Protocol (RTP) ports on remote endpoints by monitoring which RTP streams transmitted from the Cisco IPVC 35xx MCU are not heard at the endpoint.

The Cisco IPVC 35xx MCU identifies inactive RTP ports by bounced-back Internet Control Message Protocol (ICMP) error packets from remote endpoints (for example, "Unreachable Host" or "Unreachable Destination").

If this option is not selected, the Cisco IPVC 35xx MCU ignores ICMP error packets.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Settings** tab.

Step 3   Click the **Advanced** button.

Step 4   Select the **Disconnect participants on communication (ICMP) failure** check box.

Step 5   In the **Disconnect on** field, make one of the following sections:

- **Audio failure**—The call disconnects only if the audio connection fails. The call continues if the video connection fails and the audio connection remains. This is the default setting.

- **Audio or video failur**e—The call disconnects if either the audio or video connection fails.

Configuring the NetSave Feature

With the NetSave feature, you can configure the Cisco IPVC 35xx MCU to signal that endpoints should stop sending video when the participant image does not appear in the conference view. This feature reduces unnecessary bandwidth usage on the network.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Settings** tab.

Step 3   Click the **Advanced** button.

Step 4   Select the **NetSave - save video of non-displayed participants** check box.

Sending Advanced Commands

In the Advanced section of the Settings tab, you can send text-based commands used for the enhanced control of the Cisco IPVC 35xx MCU. Advanced commands are not case-sensitive.

Table 3-7 lists all available advanced commands.

Table 3-7   List of Available Advanced Commands

Command	Description	Parameters	Default
Conference control Web refresh interval	Indicates the length of time (in seconds) after which the Conference Control interface refreshes automatically.		10
DTMF forwarding **Note** This command applies only to Release 4.1.	Indicates the target of DTMF forwarding.	**to all**—All endpoints in the conference. **to gateways**—To gateways only. **to none**—DTMF is disabled.	to none
First audio announcement interval (msec)	Indicates the length of time (in milliseconds) between the start of the conference and the first audio announcement.		Disabled

Table 3-7   List of Available Advanced Commands

Command	Description	Parameters	Default
Font align	Determines whether text overlay (TOL) on a video screen is positioned away from picture borders.	**All**—Text positioned away from horizontal and vertical borders. **Horizontal**—Text positioned away from horizontal borders and centered horizontally. **Vertical**—Text positioned away from vertical borders and centered vertically. **None**—Text is always positioned bottom center.	All
G.728 Mode	Determines the form of encoding for the G.728 audio codec RTP header.	Non-standard—For use if you experience audio problems when using VCON endpoints with the G.728 audio codec. Standard—For normal G.728 use with all endpoints except VCON products.	
H323 hide stack	Disables H.323 stack prints.		
H323 show stack	Enables H.323 stack prints. These print the protocol stack info and errors and are useful for debugging stack issues		
H323 show status	Prints a snapshot of H.323 stack-related information.		
Handle DTMF after XML notification **Note** This command applies only to Release 4.1.	Instructs the Cisco IPVC 35xx MCU to send DTMF signals to an external server and other specified destinations.	**no**— Cisco IPVC 35xx MCU sends DTMF signals to the external server only. **yes**— Cisco IPVC 35xx MCU sends DTMF signals to the external server and to the destination set by the DTMF forwarding advanced command.	

Table 3-7   *List of Available Advanced Commands*

Command	Description	Parameters	Default
Notify level	Sets the Cisco IPVC 35xx MCU log notify level filter	**Fatal**— Cisco IPVC 35xx MCU cannot continue to provide service (unrecoverable error). **Error**—User functionality problem (for example, call connect failure or no resources available). **Warning**—User functionality problem but the Cisco IPVC 35xx MCU can continue to provide service. **Info**—Status prints for Customer Support use. **Advanced**—Like **Info** but more detailed. **Debug 1** through **Debug 4**—Debug levels.	Debug 3
QualiVision Settings show	Enables the QualiVision Settings section in the Settings tab.		The QualiVision Settings section is hidden by default.
QualiVision Settings hide	Disables the QualiVision Settings section in the Settings tab.		
SCCP show stack	Enables SCCP stack prints. These print the protocol stack info and errors and are useful for debugging stack issues.		
SCCP hide stack	Disables SCCP stack prints.		
SCCP show status	Prints a snapshot of SCCP stack related information.		
Set MTU size	Determines the maximum packet size across the network.		1500

Table 3-7   *List of Available Advanced Commands*

Command	Description	Parameters	Default
Set terminal baud rate	Sets the baud rate of a serial terminal.	**High (57600)** **Low (9600)**	Low (9600)
Use EMP	Determines whether a conference opens on a local MP unit or on an EMP.	**Always**—Conference always opens on EMP. **Only when needed**—Conference opens on local MP unit unless EMP resources are required.	

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Settings** tab.

Step 3   Click the **Advanced** button.

Step 4   Click **Commands**.

The Advanced Commands dialog box appears.

Step 5   In the **Command** field, enter a command or choose one from the **Available Commands** field.

Step 6   In the **Parameters** field, enter a parameter value for the command (where applicable) or choose one from the **Available Parameters** field.

Step 7   Click **Send**.

The results of the advanced command appear in the Results field, indicating whether or not the Cisco IPVC 35xx MCU received and executed the command. If you send an invalid command, a "bad parameter" or "NOT FOUND" message appears.

Opening a Telnet Terminal

In the Advanced section of the Settings tab, you can open a Telnet terminal to log error and troubleshooting information.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Settings** tab.

Step 3   Click the **Advanced** button.

Step 4   Click **Telnet**.

Step 5   A separate browser opens with a Telnet terminal. When you finish with your Telnet session, click **Disconnect**.

Configuring QualiVision Settings

In the QualiVision Settings section of the Settings tab, you can configure policies for filtering video update requests from endpoints connected to conferences hosted on the Cisco IPVC 35xx MCU.

Note We recommend that you use the default settings for channel classification and intra-frame (a method of video encoding) limiting options.

This QualiVision feature provides improved support for networks with packet loss rates of up to seven percent. The QualiVision feature enables the Cisco IPVC 35xx MCU to control the video quality and limit the demand on video processing resources by endpoints with poor connections. Indications appear for each participant in the Conference Control interface to signify which endpoint has a poor quality connection that is affecting the overall video quality of the conference. Administrators can use these indications to directly investigate the source of poor network connections.

The following sections detail QualiVision configuration:

- Understanding VFU Classification, page 3-24
- Configuring Outgoing Channel Classification, page 3-25
- Configuring Incoming Channel Classification, page 3-26
- Configuring Intra-frame Limiting Settings, page 3-26

Understanding VFU Classification

The Cisco IPVC 35xx MCU analyzes the frequency of the Video Fast Update (VFU) requests that each endpoint sends and then ranks each endpoint into video quality classes. Each ranking represents a video quality status. A high frequency of VFU requests indicates a poor connection between the endpoint and the Cisco IPVC 35xx MCU. When endpoints enter a conference, the Cisco IPVC 35xx MCU automatically ranks them with a quality class. Throughout the duration of the connection, the Cisco IPVC 35xx MCU recalculates the class based on the analysis of VFU request frequency. Based on the calculated class, the Cisco IPVC 35xx MCU filters VFU requests so that MPs do not create too many intra-frames (a method of video encoding) damaging video quality for other conference participants.

Table 3-8 lists VFU endpoint classes.

Table 3-8   VFU Endpoint Classes

Endpoint Classification (Video Quality)	Corresponding Packet Loss (%)
Class A (good)	< 0.2
Class B (medium)	0.2 to 2
Class C (poor)	> 2

In the Participant List tab of the Conference Control interface, the Cisco IPVC 35xx MCU displays a warning icon next to every endpoint that suffers from packet loss or that the Cisco IPVC 35xx MCU has assigned a high endpoint classification value. Table 3-9 lists the warning icons.

Table 3-9   Video Quality Warnings

Outgoing Channel VFU Classification	Incoming Channel Corresponding Packet Loss (%)	Icon
Class A (good)	< 0.2	None
Class B (medium)	0.2 to 2	⚠️
Class C (poor)	> 2	❗

Configuring Outgoing Channel Classification

In the QualiVision section of the Settings tab, you can configure outgoing channel classification. These settings affect the display of endpoint status in the Conference Control interface.

Before You Begin

You must first enable the "QualiVision Settings show" advanced command. See the for more information.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Settings** tab.

Step 3   Click the **QualiVision Settings** button.

Step 4   From the **Algorithm strength** field, select the required algorithm strength:

- **strong**
- **normal**
- **weak**

Step 5   To enable QualiVision on incoming channels (from the Cisco IPVC 35xx MCU to endpoints), select the **Enable QualiVision on outgoing channels (MCU -> Endpoints)** check box.

Step 6   To configure outgoing channel classification settings, click **Outgoing channel classification**.

The Outgoing channel classification dialog box appears.

Step 7   For each video quality class—A (Good), B (Medium), and C (Poor)—in the **Threshold for next class (VFU requests per 10 sec)** field, enter the maximum number of VFU requests every 10 seconds tolerated in the class before the video quality class changes. Enter a whole number from 1 to 20.

Step 8   For each video quality class, in the **Times to cross threshold before changing class** field, enter the number of times that the threshold must be crossed before the Cisco IPVC 35xx MCU moves an endpoint to the next classification level. Enter a value from 1 to 30.

Step 9   Click **OK**.

■ Configuring Cisco IPVC 35xx MCU Settings

Configuring Incoming Channel Classification

In the QualiVision section of the Settings tab, you can configure incoming channel classification. These settings affect the display of endpoint status in the Conference Control interface.

Before You Begin

You must first enable the QualiVision Settings show advanced command. See the "Sending Advanced Commands" section on page 3-20 for more information.

Procedure

Step 1 In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2 Click the **Settings** tab.

Step 3 Click the **QualiVision Settings** button.

Step 4 To enable QualiVision on incoming channels (endpoints to the Cisco IPVC 35xx MCU), select the **Enable QualiVision on incoming channels (Endpoints -> MCU)** check box.

Step 5 Click **Incoming channel classification** to configure incoming channel classification settings.

The Incoming channel classification dialog box appears.

Step 6 For each video quality class—A (Good), B (Medium), and C (Poor)—in the **Threshold for next class (% packet loss during 10 sec)** field, enter the maximum percentage of packet loss every ten seconds tolerated in the class before the video quality changes. Enter a whole number from 1 to 20.

Step 7 For each video quality class, in the **Times to cross threshold before changing class** field, enter the number of times the threshold must be crossed before the Cisco IPVC 35xx MCU moves an endpoint to the next classification level. Enter a whole number from 1 to 30.

Step 8 Click **OK**.

Configuring Intra-frame Limiting Settings

Endpoints that suffer from packet loss typically request intra-frames, which is a method of video encoding. A high rate of intra-frames causes video image flickering connected to the output stream. You can configure the rate of intra-frames that the Cisco IPVC 35xx MCU sends according to the endpoint class and avoid a flickering image when an endpoint requests a fast update.

Before You Begin

You must first enable the QualiVision Settings show advanced command. See the "Sending Advanced Commands" section on page 3-20 for more information.

Procedure

Step 1 In the Administrator interface, click the **MCU** button (If not already selected).

Step 2 Click the **Settings** tab.

Step 3 Click the **QualiVision Settings** button

Step 4 Select the **Limit the rate of intra frames sent in response to "Video Fast Update (VFU)" requests** check box.

Step 5   Click **Intra frame limiting settings**.

The Intra frame limiting dialog box appears.

Step 6   In the **Limit the rate of intra frames sent, according to the endpoint class** field, enter values (representing seconds) for each video quality class (A, B, and C).

Step 7   Click **OK**.

Viewing Registered MPs

In the Registered MPs tab, you can view the list of Media Processors (MP) currently registered with the Cisco IPVC 35xx MCU and edit settings.The Registered MPs tab lists all registered MPs in table format with the following columns and fields:

- Type—This column displays the type of MP unit registered with the current Cisco IPVC 35xx MCU. The following types of MP can appear in this column:

  - MP—The MP component of a Cisco IPVC 35xx MCU or a Cisco IPVC 35xx MCU where the Multipoint Controller (MC) component is disabled. The MP unit performs basic media processing such as audio transcoding, video processing, and video switching.

  - EMP—Enhanced Media Processor (EMP) unit performing advanced media processing such as video processing and video switching.

  - RMM—Rate Matching Module (RMM) unit performing media processing such as video bandwidth and picture size transcoding.

  - DCS—Cisco IPVC 3540 Application Server (AS) Module for Data Collaboration Server (DCS) providing T.120 data collaboration services.

- IP Address—This column displays the IP address of the device on which the MP operates.

- Description—This column displays a user-defined description of the MP.

- Total—This field displays the total number of MP units currently registered.

Note   In Release 4.1 only, the Cisco IPVC 35xx MCU rejects an Enhanced Media Processor (EMP) without the correct version if it tries to register with it. Notice of this rejection appears in the Event Log tab.

Related Topics

- Configuring Registered MPs, page 3-27

Configuring Registered MPs

In the Registered MPs tab, you can configure the local MP component of the Cisco IPVC 35xx MCU and other MP units that it manages. You can configure settings for managing audio and video processing, and audio codec transcoding preferences.

Procedure

Step 1   In the Administrator interface, click **MCU** (if not already selected).

Step 2   Click the **Registered MPs** tab.

Step 3   Click the registered MP you want to configure and then click **Go to**.

The **MP Settings** dialog box appears.

Step 4   Make sure the **Basics** tab is selected. In the Basics tab, you configure the media processing capabilities of the current device, including registration settings and audio and video processing support. The MCU IP address and MCU port appear in those respective fields. You cannot configure these settings on a local Cisco IPVC 35xx MCU.

Step 5   To enable audio processing on the current device, select the **Audio processing enabled** check box.

Step 6   If you did not enable audio processing in step 5, skip to step 7. Otherwise, in the **Audio packet size** field, choose the size in milliseconds of outgoing audio packets from the following options:

- **small (20-30 ms)**—Selecting small packets causes shorter network delays, but more network traffic and higher CPU usage.

- **large (60 ms)**—Selecting large packets causes longer network delays, but less network traffic and lower CPU usage.

Step 7   To enable video processing on the current device, select the **Video processing enabled** check box.

Step 8   In the **RTP base port** field, enter the Real-Time Transport Protocol (RTP) port number on which media communications are conducted. You can enter a port number from 1 to 65535.

Step 9   Click the **Media Modes** tab. In the Media Modes tab, you manage audio transcoding of supported audio codecs on registered MP units.

Step 10   In the **Reserve transcoders for G.722.1 calls** field, choose one of the following numbers to define the maximum number of G.7221 calls for which audio transcoders are reserved:

- **0**
- **2**
- **4**
- **6**
- **8**
- **10**
- **12**
- **14**

The Max calls for each other codec field displays the maximum number of transcoded calls for each call type. The relative number of transcoded calls for each codec is automatically changed when you change the maximum number of transcoded G.722.1 calls according to the total number of available transcoders.

Step 11   Click **Upload**.

Related Topics

-

About Protocols and the Cisco IPVC 35xx MCU

In the Protocols tab, you can configure the Cisco IPVC 35xx MCU to work with H.323, Session Initiation Protocol (SIP), and Skinny Client Control Protocol (SCCP) call-routing devices. The following sections detail the three types of call-routing devices you can configure the Cisco IPVC 35xx MCU to work with:

Configuring H.323 Gatekeeper Settings

In the Protocols tab, you can view and configure settings for H.323 gatekeeper call routing devices. The following sections detail the tasks you can perform in the Protocols tab:

Viewing H.323 Gatekeeper Settings

In the Protocols tab, you can view details of the current H.323 gatekeeper through which video calls route to the Cisco IPVC 35xx MCU.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Protocols** tab.

Step 3   Make sure the **H.323** button is selected.

The H.323 section of the Protocols tab displays the following settings:

- Description—User description of the current H.323 gatekeeper profile.
- Gatekeeper Address—IP address of the current H.323 gatekeeper.
- Status—Status of the current H.323 gatekeeper: enabled or disabled.
- Servicing Gatekeeper—IP address and port number of the gatekeeper that the current H.323 interface uses.
- Total—Indicates the total number of H.323 gatekeepers currently defined.

Editing H.323 Gatekeeper Protocol Configuration

In the Protocols tab, you can edit the protocol settings of an H.323 gatekeeper to configure how the Cisco IPVC 35xx MCU and gatekeeper interact.

Procedure

Step 1 In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2 Click the **Protocols** tab.

Step 3 Make sure the **H.323** button is selected.

Step 4 In the **H.323 Protocol Configurations** area, click a H.323 gatekeeper and then click **Edit**.

The Edit H.323 Protocol Configurations dialog box appears.

Step 5 Select the **Activate protocol settings** check box to enable the Cisco IPVC 35xx MCU to operate with the H.323 gatekeeper to which this profile is configured.

Step 6 In the **Description** field, enter a description of the protocol configuration. This appears in the H.323 Protocol Configurations area of the Protocols tab.

Step 7 In the **Gatekeeper Address** field, enter the IP address of the gatekeeper.

Step 8 In the **Gatekeeper Port** field, enter the port number of the gatekeeper. The default port is 1719.

Step 9 Select the **Strip local gatekeeper zone prefix if it appears in incoming cells** check box if you want the Cisco IPVC 35xx MCU to strip the gatekeeper zone prefix from the dialed string of an incoming call. You can use this feature when the gatekeeper does not perform zone stripping.

Step 10 If you did not perform step 9, skip to step 11. Otherwise, in the **Local Zone Prefix** field, enter the gatekeeper zone you want to strip.

Step 11 Click **Upload**.

⚠

Caution   Changing gatekeeper settings does not reset the Cisco IPVC 35xx MCU, but might disconnect active calls.

Tips

In the Edit H.323 Protocol Configurations dialog box, you can click **Go to Gatekeeper** to connect to a third-party gatekeeper that uses a web interface.

Configuring Advanced H.323 Gatekeeper Protocol Settings

In the Protocols tab, you can configure advanced settings for Cisco IPVC 35xx MCU communication with an H.323 gatekeeper.

Before You Begin

Make sure the basic H.323 gatekeeper protocol settings are correct. See the "Editing H.323 Gatekeeper Protocol Configuration" section on page 3-29 for more information.

Procedure

Step 1 In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2 Click the **Protocols** tab.

Step 3 Make sure the **H.323** button is selected.

Step 4 In the **H.323 Protocol Configurations** area, click a H.323 gatekeeper and then click the **Edit** button.

The Edit H.323 Protocol Configurations dialog box appears.

Step 5   Make sure that the **Activate protocol settings** check box is selected

Step 6   Click **Advanced H.323 Settings**.

The Edit H.323 Protocol Configuration dialog box appears.

Step 7   In the **RAS Port** field, enter the port on which the Cisco IPVC 35xx MCU conducts RAS registration messaging with the gatekeeper. The default port is 2719.

Step 8   In the **Signalling Port** field, enter the port on which the Cisco IPVC 35xx MCU carries call signalling messages to and from the gatekeeper. The default port is 2720.

Step 9   In the **Registration refresh every** field, enter the interval (in seconds) between registrations of the Cisco IPVC 35xx MCU to the gatekeeper. The default value is 60 seconds.

Step 10   In the **MCU Registration Mode** field, choose the mode with which the Cisco IPVC 35xx MCU registers with the gatekeeper from the following options:

- **MCU**—Use this setting when registering with a third-party gatekeeper.

- **Gateway**—Use this setting when registering with a Cisco gatekeeper. This is the default setting.

Step 11   Select the **Enable H.239** check box to enable support for dual-video using the H.239 protocol.

⚠
Caution   We recommend that you disable this feature if communications are to be established with endpoints that do not support H.245 generic capabilities (endpoints based on H.323 version 2 or earlier) as this might cause the endpoints to fail upon receiving these capability exchanges.

Step 12   Select the **Enable Fast Start** check box to speed up the connection time between the Cisco IPVC 35xx MCU and incoming calls received through the gatekeeper. Channel setup messages are encapsulated within Q.931 setup messages. When you enable this option, the Cisco IPVC 35xx MCU offers Fast Start channels to any outgoing call and attempts to select from channels offered in incoming calls.

Step 13   Select the **Enable generic audio capabilities (required for G.722.1 support)** check box to enable H.245 generic capabilities exchange used for G.722.1, H.264, and H.239 capability exchange.

⚠
Caution   We recommend that you disable this feature if communications are to be established with endpoints that do not support H.245 generic capabilities (endpoints based on H.323 version 2 or earlier) as this might cause the endpoints to fail upon receiving these capability exchanges.

Step 14   Select the **Enable H.245 tunneling** check box to enable H.245 tunneling during call setup and connection between the Cisco IPVC 35xx MCU and incoming calls received through the gatekeeper.

✎
Note   The H.245 tunneling feature works only with endpoints and gatekeepers that support H.245.

Step 15   Click **OK**.

Integrating SIP with the Cisco IPVC 35xx MCU

This section describes how to configure the Cisco IPVC 35xx MCU and use different dialing plans for working in a Session Initiation Protocol (SIP) environment. The section describes the following topics:

- Understanding SIP Architecture, page 3-32
- Viewing SIP Proxy Settings, page 3-33
- Configuring SIP Proxy Settings, page 3-34
- About the Cisco IPVC 35xx MCU Dial Plan, page 3-35

Understanding SIP Architecture

A SIP environment is composed of domains. Each domain has a name such as sip.radvision.com. Every domain usually has a SIP proxy, which handles the SIP traffic both within the domain and to other domains, similar to the zone concept in H323.

A domain also includes SIP-compliant endpoints called User Agent Clients (UACs) and a SIP registrar which maintains UAC registrations in the domain Location Service that stores registrations. When the proxy receives invite requests from other UACs, it consults the Location Service in order to find the invited party before sending the invitation to the appropriate destination.

The following events, shown in Figure 3-3, demonstrate the basic interactions in a SIP environment:

- Registration—The SIP Registrar Server receives a Register request from a UAC. The Registrar forwards each request to the Location Service to update the database.
- Invite—A SIP Invite message arrives to the proxy. The proxy consults with the Location Service to obtain the IP to which it should route the Invite message. The proxy can also consult with a DNS server instead of a Registrar.

Figure 3-3   *SIP Domain Topology*
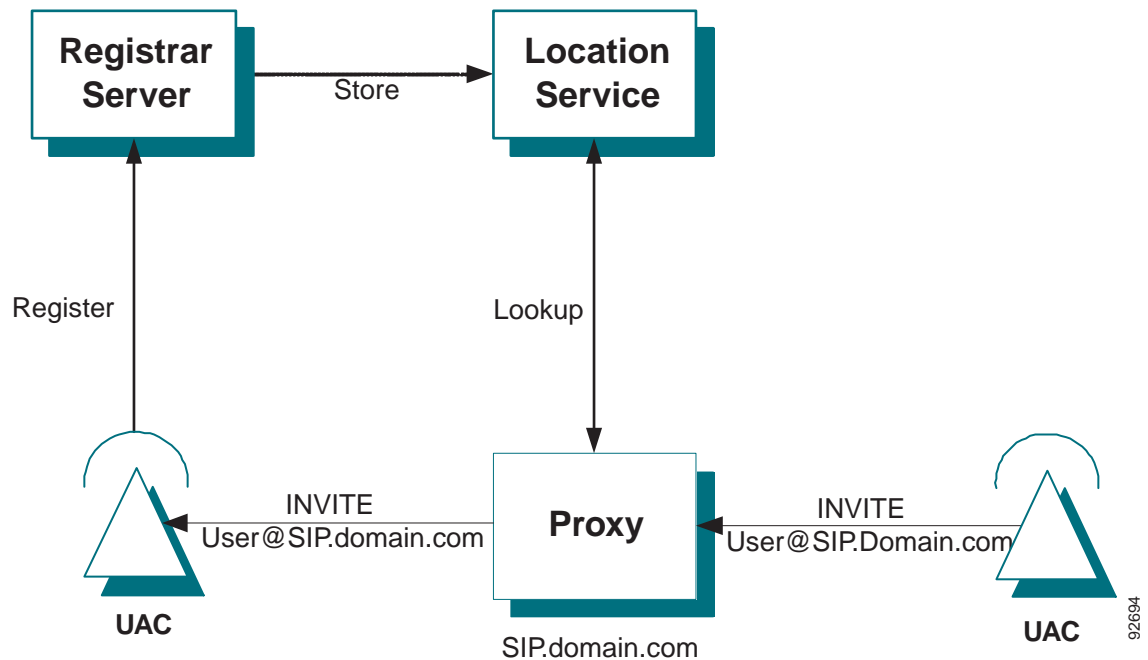
Viewing SIP Proxy Settings

The SIP section of the Protocols tab displays addressing details of the current SIP proxy through which video calls from SIP endpoints are routed to the Cisco IPVC 35xx MCU.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Protocols** tab.

Step 3   Click the **SIP** button.

The SIP section of the Protocols tab displays the following settings:

- Description—Description of the SIP proxy profile.

- Proxy Address—IP address and port number of the SIP proxy.

- Status—Status of the current SIP proxy: enabled or disabled.

- Servicing/Registrar—IP address, domain name, or SIP Uniform Resource Identifier (URI) of the registrar providing address translation for the SIP proxy.

- Total—Indicates the total number of SIP proxies with which the Cisco IPVC 35xx MCU operates.

Configuring SIP Proxy Settings

You can edit configuration settings for SIP registrar profiles which set how the Cisco IPVC 35xx MCU and registrar interact.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Protocols** tab.

Step 3   Make sure the **SIP** button is selected.

Step 4   In the **SIP Protocol Configurations** area, click a SIP proxy profile and then click **Edit**.

The Edit SIP Protocol Configurations dialog box appears.

Step 5   Select the **Enable** check box to enable Cisco IPVC 35xx MCU communication with the SIP proxy.

Step 6   In the **Description** field, enter a description of the protocol configuration.

Step 7   In the **Proxy Address** field, enter the IP address of the SIP proxy.

Step 8   In the **Proxy port** field, enter the communication port number of the SIP proxy.

Step 9   Select the **Use registrar** check box for the Cisco IPVC 35xx MCU to register the following information with the SIP proxy server registrar:

- Cisco IPVC 35xx MCU name—Registers the Cisco IPVC 35xx MCU alias specified in the MCU Identifier field of the Basics section of the Settings tab. See the "Setting the Cisco IPVC 35xx MCU Identifier Basic Setting" section on page 3-5 for more information.

- Cisco IPVC 35xx MCU services—Registers Cisco IPVC 35xx MCU services.

- Conference ID—Registers the conference ID of existing conferences when Register conference ID is also selected in the Conference Mgmt section of the Settings tab (See the "Configuring Cisco IPVC 35xx MCU Conference Management Settings" section on page 3-6 for more information). This enables the SIP proxy to route calls from SIP endpoints to conferences on the Cisco IPVC 35xx MCU that do not include the Cisco IPVC 35xx MCU domain name in the dialed string.

When you select this option, the SIP proxy address is also used as the registrar address.

Step 10   If you did not perform step 9, skip to step 11. Otherwise, in the **Registrar communication type** field, select the transport connection type for sending registration requests to the registrar according to the type supported by the SIP proxy: **UDP** or **TCP**.

> **Note**   Some SIP proxies only accept registration requests using a secure Transmission Control Protocol (TCP) communication connection type.

Step 11   In the **Default Domain** field, enter the SIP domain name of the Cisco IPVC 35xx MCU as defined on the following SIP servers:

- Microsoft RTC servers—The domain name registered on the DNS server or Real-time Communications (RTC) proxy list.

- Other SIP servers—The proxy domain name.

> **Note**   When the domain name is not specified in the dialed string of an outgoing call, the default domain name is appended on the string. For registering, the Cisco IPVC 35xx MCU appends the default domain to each service and registers the services to the registrar. For dialing, the Cisco IPVC 35xx MCU appends the default domain when dialing out a SIP call from the Cisco IPVC 35xx MCU using just the remote party number or user name (For example: @cisco.com or @default.domain).

Step 12   In the **Local signalling port** field, enter the signalling port number on which the Cisco IPVC 35xx MCU communicates with the SIP proxy.

Step 13   In the **Out transport connection type** field, select the transport connection type for call signalling according to the type supported by the SIP proxy: **UDP** or **TCP**.

> **Note**   Some SIP proxies only accept calls using a secure TCP connection type.

Step 14   In the **Out contact header type** field, select the conference and Cisco IPVC 35xx MCU addressing format of the contact information sent in the header of the outgoing call:

- Microsoft RTC Server—Default SIP domain.
- Other servers—Local signalling IP.

Step 15   Select the **Enable Video Fast Update** check box to support Video Fast Update (VFU) requests from SIP endpoints and initiate requests to the endpoints.

Step 16   Click **Upload**.

About the Cisco IPVC 35xx MCU Dial Plan

You can configure the Cisco IPVC 35xx MCU on a SIP network in one of the following two ways:

- The Cisco IPVC 35xx MCU functions as a User Agent Client (UAC) which provides video, voice, and data conferencing services.
- The Cisco IPVC 35xx MCU is defined as a separate domain that provides conferencing services.

The following sections describe these configurations:

About Outgoing Calls from the Cisco IPVC 35xx MCU

Making outgoing calls from the Cisco IPVC 35xx MCU is the same whether it operates as a UAC or as a separate SIP domain. All Cisco IPVC 35xx MCU outgoing SIP messages are sent through the proxy. The proxy activates an address resolution algorithm by consulting with a registrar or a DNS server or any other location server and routes the message to the correct destination.

Note   If the user does not specify a domain in the dialing string, the Cisco IPVC 35xx MCU appends the default domain to the dialed string. You can configure the default domain in the SIP section of the Protocols tab. See the "Configuring SIP Proxy Settings" section on page 3-34 for more information.

About Incoming Calls to the Cisco IPVC 35xx MCU

The Cisco IPVC 35xx MCU dial plan for incoming calls varies according to whether the Cisco IPVC 35xx MCU is configured as a UAC registered to the domain registrar or as a separate SIP domain.

Note   Whether working as a UAC or separate SIP domain, you can dial into the Cisco IPVC 35xx MCU from a UAC by dialing a conference.id@mcu.ip.address URI and the call should always reach the Cisco IPVC 35xx MCU.

Configuring the Cisco IPVC 35xx MCU as a UAC

In the Protocols tab, you can configure the Cisco IPVC 35xx MCU to function as a UAC. When configured as a UAC, the Cisco IPVC 35xx MCU registers all services and conferences with a registrar. We recommend that you configure the Cisco IPVC 35xx MCU as a UAC when working with a scheduler or in an environment that does not require ad hoc conference creation. In this configuration, the UAC can only dial directly into the Cisco IPVC 35xx MCU by using a conference ID that has previously registered with the registrar.

Ad hoc conference creation using conference services, familiar in an H.323 environment, is not supported in a SIP environment. When a SIP UAC dials into the Cisco IPVC 35xx MCU to a conference that does not yet exist, the proxy cannot resolve the Cisco IPVC 35xx MCU address because the dialed conference ID is not registered with a registrar.

The Cisco IPVC 35xx MCU registers each Cisco IPVC 35xx MCU service and conference using the default domain defined in the Cisco IPVC 35xx MCU SIP configuration and SIP proxy server as follows:

- Service: 60@radvision.com
    - 60—Cisco IPVC 35xx MCU service prefix
    - @radvision.com—Cisco IPVC 35xx MCU default domain
- Conference: 601234@radvision.com
    - 601234—Cisco IPVC 35xx MCU conference ID (service prefix + unique conference identifier)
    - @radvision.com—Cisco IPVC 35xx MCU default domain on which the conference is hosted.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Protocols** tab.

Step 3   Make sure the **SIP** button is selected.

Step 4   In the **SIP Protocol Configurations** area, click a SIP proxy settings profile and then click **Edit**.

The Edit SIP Protocol Configurations dialog box appears.

Step 5   Select the **Use registrar** check box.

Step 6 In the **Default Domain** field, enter the default domain name as defined in the SIP proxy server.

Step 7 Click **Upload**.

Step 8 Click the **Settings** tab and then click the **Conference Mgmt** button.

Step 9 Make sure that the **Register conference ID** check box is selected.

> **Note** The Cisco IPVC 35xx MCU must use the registrar to register conference IDs. Conferences cannot be found if the registrar has no record that they exist, causing all calls to conferences to fail.

Configuring the Cisco IPVC 35xx MCU to Perform as a Separate SIP Domain

You can configure the Cisco IPVC 35xx MCU to perform as a separate domain within the default domain. The default domain is the domain in which the Cisco IPVC 35xx MCU operates as defined in the SIP proxy server. Every SIP request that the proxy receives that ends with the unique domain name of the Cisco IPVC 35xx MCU routes directly to the Cisco IPVC 35xx MCU. The Cisco IPVC 35xx MCU then directs the call to the appropriate conference. Pre-registering the conference IDs with the registrar is not required.

Procedure

Step 1 In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2 Click the **Protocols** tab.

Step 3 Make sure the **SIP** button is selected.

Step 4 In the **SIP Protocol Configurations** area, click a SIP proxy settings profile and then click **Edit**.

The Edit SIP Protocol Configurations dialog box appears.

Step 5 In the **Default Domain** field, enter the name of the domain in which the Cisco IPVC 35xx MCU operates.

For example, enter:

Cisco.com.

Step 6 Configure the unique domain name of the Cisco IPVC 35xx MCU in the proxy internal routing tables (if supported) or in the relevant DNS server:

- For proxy internal routing tables, configure a rule such as:

    Every URI of type *(any number)@mcu.cisco.com should be routed to the Cisco IPVC 35xx MCU IP address.

- For a DNS server, define a new rule entry of mcu.cisco.com. The address of this entry is the Cisco IPVC 35xx MCU IP.

> **Note** Make sure that the Cisco IPVC 35xx MCU domain configured in the proxy is different from the default domain. If the Cisco IPVC 35xx MCU default domain is cisco.com, then configure the Cisco IPVC 35xx MCU domain as mcu.cisco.com.

Configuring the Cisco IPVC 35xx MCU to Use Cisco CallManager SCCP

To set up the Cisco IPVC 35xx MCU to use Cisco CallManager which uses the Skinny Client Control Protocol (SCCP) protocol, you must enable the Cisco IPVC 35xx MCU to support SCCP. Then you must identify the Trivial File Transfer Protocol (TFTP) server that you want the Cisco IPVC 35xx MCU to use. This allows the Cisco IPVC 35xx MCU to contact the Cisco CallManager and obtain configuration information specific to that Cisco CallManager. You must also set pertinent Cisco IPVC 35xx MCU parameters for proper operation. You set the Cisco IPVC 35xx MCU-based parameters in the Administrator interface and you can set the Cisco CallManager-based parameters in the Cisco CallManager. The Cisco CallManager-based parameters upload to the Cisco IPVC 35xx MCU and appear in the Administrator interface after contact is made.

> **Note** When you boot up, the Cisco IPVC 35xx MCU reports EMP resources associated with SCCP conferences to Cisco CallManager. These resources are reserved and subtracted from the remaining Cisco IPVC 35xx MCU resources available to H.323 conferences.

Viewing SCCP Protocol Configurations

In the Protocols tab, you can view existing SCCP protocol configurations.

Procedure

Step 1 In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2 Click the **Protocols** tab.

Step 3 Click the **SCCP** button.

The SCCP section of the Protocols tab displays the following settings:

- Description—Indicates that this protocol is SCCP.
- Status—The current status of the SCCP protocol for this device.
- Servicing CallManager—The IP address of the Cisco CallManager that the Cisco IPVC 35xx MCU uses.
- Servicing TFTP—The IP address of the primary TFTP server that the Cisco IPVC 35xx MCU uses
- Total—The total number of SCCP entries.

Configuring the SCCP Protocol

In the Protocols tab, you can configure the Cisco IPVC 35xx MCU to support SCCP in Cisco CallManager.

Procedure

Step 1 In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2 Click the **Protocols** tab.

Step 3   Click the **SCCP** button.

Step 4   Click the Cisco CallManager entry for which you want to set parameters and then click **Edit**.

The Edit SCCP Protocol Configuration dialog box appears.

Step 5   Select the **Enable** check box to allow the Cisco IPVC 35xx MCU to support the SCCP protocol.

Step 6   In the **Active SCCP service prefix** field, enter the prefix assigned to the Cisco IPVC 35xx MCU service that you want the Cisco CallManager to use.

> **Note**   A default service prefix is automatically entered in this field. If you want to use this service, make sure that this is a valid service prefix for your network environment. See the "About Services" section on page 3-42, for more information about creating Cisco IPVC 35xx MCU services.

Step 7   In the TFTP Servers section, identify the TFTP server that you want the Cisco IPVC 35xx MCU to use.

> **Note**   This information appears automatically when you use the terminal emulator to set a TFTP server address. You can edit this information or add a different TFTP server.

    a.   In the TFTP Servers section, click **Add**.

       The Add TFTP Server dialog box appears.

    b.   In the **IP Address** field, enter the IP address of the TFTP server you want the Cisco IPVC 35xx MCU to use to contact the Cisco CallManager.

    c.   In the **Port** field, enter the port number that you want the Cisco IPVC 35xx MCU to use to communicate with the TFTP server.

    d.   Choose **OK** to save these changes and close the Add TFTP server dialog box.

Step 8   Select the **Perform MCU reset on CallManager Reset message** check box to have the Cisco IPVC 35xx MCU reset when it receives a reset message from the Cisco CallManager. The default setting is unselected.

> **Caution**   The Cisco IPVC 35xx MCU immediately drops calls that are in process when the Cisco CallManager sends a reset message.

Step 9   Click **OK** to save your changes.

Viewing the Edit SCCP Protocol Configuration Dialog Box

In the Edit SCCP Protocol Configuration dialog box, you can configure the Cisco IPVC 35xx MCU to communicate with and support the Cisco CallManager, and to view and set parameters that are common to both. The information in this dialog box is shared between the Cisco IPVC 35xx MCU and Cisco CallManager. Some fields relate to Cisco IPVC 35xx MCU-based parameters, while other fields relate to Cisco CallManager-based parameters. You must configure the fields for the Cisco IPVC 35xx MCU-based parameter in this page.

Although you can configure fields that host Cisco CallManager-based parameters in this page, we recommend that you configure those parameters in the Cisco CallManager conference bridge profile that you create for this. Those parameters upload to the Cisco IPVC 35xx MCU when communication between the two devices begins.

Table 3-10 describes the elements that appear in the Edit SCCP Protocol Configuration dialog box.

Table 3-10   Edit SCCP Protocol Configuration Dialog Box

Field	Description
Enable	Select this check box to allow the Cisco IPVC 35xx MCUto support the SCCP protocol.
Active SCCP service prefix	Enter a value you want to use for the service prefix.
TFTP section	
IP Address	Displays IP addresses of TFTP servers that are available for the Cisco IPVC 35xx MCU to use.
Port	Displays the listening port that the available TFTP servers use.
Buttons	**Add**—Click to launch the Add TFTP Server dialog box where you enter the following settings: • IP address—The IP address of the TFTP server you want the Cisco IPVC 35xx MCU to use. • Port—The port number that you want the Cisco IPVC 35xx MCU to use to communicate with the TFTP server. **Edit**—Click to launch the Edit TFTP Server dialog box where you can edit the following settings: • IP address: The IP address of the TFTP server that the Cisco IPVC 35xx MCU is using. • Port—The port number that the Cisco IPVC 35xx MCU is using to communicate with the TFTP server. **Delete**—Click to delete a selected TFTP server.
Cisco CallManagers section	
IP Address	Displays the IP address of Cisco CallManagers that the Cisco IPVC 35xx MCU supports as a device.
Port	Displays the Cisco CallManager port number through which the Cisco IPVC 35xx MCU communicates with the Cisco CallManager.

Table 3-10   Edit SCCP Protocol Configuration Dialog Box

Field	Description
Buttons	**Add**—Choose to launch the Add CallManager dialog box where you enter the following settings: • IP address—Enter the IP address of the Cisco CallManager that you want the Cisco IPVC 35xx MCU to use. • Port—Enter the port number that you want the Cisco IPVC 35xx MCU to use to communicate with the Cisco CallManager. **Edit**—Choose to launch the Edit CallManager dialog box where you can edit the profile of the selected Cisco CallManager. **Delete**—Click to delete the selected Cisco CallManager.
Perform MCU reset on Cisco CallManager reset message	Select this check box to configure the Cisco IPVC 35xx MCU to reset when it receives a reset message from Cisco CallManager.
Control Channel section	
Local port base	Enter a value for the communication port that you want the Cisco IPVC 35xx MCU to use to communicate with the Cisco CallManager. You can use values between 11000 and 16000. The default value is 11000. **Note** You must set this value in the Cisco CallManager also.
Priority (0-63)	Enter the Differentiated Services Code Point (DSCP) value the Cisco CallManager specifies that the Cisco IPVC 35xx MCU use for Quality of Service (QoS). You must convert the value to decimal notation.
Registration section	
Retries	Enter a value setting the number of times you want the Cisco IPVC 35xx MCU to attempt to register with the Cisco CallManager.
Initial timeout (sec)	Enter a value in seconds setting the length of time the Cisco IPVC 35xx MCU waits for a response from the Cisco CallManager before timing out on the first attempt to register.
Consequent timeout (sec)	Enter a value in seconds setting the length of time the Cisco IPVC 35xx MCU waits for a response from the Cisco CallManager before timing out on subsequent attempt to register.
Keep Alive section	

Table 3-10   Edit SCCP Protocol Configuration Dialog Box

Field	Description
Retries	Enter a value setting the number of times you want the Cisco IPVC 35xx MCU to send the Keep Alive message to the Cisco CallManager before acknowledging that the connection has failed.
Timeout (sec)	Enter a value in seconds setting the interval at which the Cisco IPVC 35xx MCU sends Keep Alive messages.
Fail Over section	
Change configuration locally	Select this check box to configure settings in the Recovery mode and Recovery timeout (sec) fields.
Recovery mode	Choose the mode with which you want the Cisco IPVC 35xx MCU to terminate calls when the connection to the Cisco CallManager fails: • **gracefully**—Allow completion of current calls. • **immediately**—Terminate conference immediately. • **timeout**—Allow all conferences to continue for the interval specified in the Recovery timeout (sec) field.
Recovery timeout (sec)	If you select **timeout** in the **Recovery mode** field, enter a value in seconds setting the length of time the Cisco IPVC 35xx MCU allows calls to continue after the connection with the Cisco CallManager fails.
OK	Choose to save changes.
Cancel	Choose to close this dialog box without saving changes.

About Services

A service is the mechanism that defines the qualities and capabilities of a conference and is identified by a prefix. You can define up to 50 different services for the Cisco IPVC 35xx MCU. In the Services tab, you can view, add, and edit conferencing service profiles for a Cisco IPVC 35xx MCU.

Each entry in the Services tab represents a different type of conferencing service. When you access the Services tab for the first time, several default services appear.

The Services tab displays the following information:

• Prefix—Displays the service prefix number incorporated into the conference ID to specify the service for the conference.

- Description—Description of the service indicating the main attributes of the service or the target use for the service.
- Status—Indicates whether the service is enabled. A service can be disabled if the Cisco IPVC 35xx MCU does not support functionality that the service requires.
- Parties—Indicates the maximum number of participants that can attend conferences using this service.
- Media—Indicates the media supported in conferences using this service: voice; video; or data.
- Bandwidth (Kbps)—Indicates the bandwidth rate (in kilobytes per second) for conferences using this service.
- Total—Indicates the total number of service types available on the current Cisco IPVC 35xx MCU.

To add a new service or configure an existing service, follow these procedures:

- Adding a Service, page 3-43 or Editing a Service, page 3-44
- Configuring Basic Service Settings, page 3-46
- Configuring Service Video Settings, page 3-47
- Configuring Service Indication Settings, page 3-48
- Configuring Service Management Settings, page 3-49
- Configuring Conference Views, page 3-50
- Configuring Service Audio Transcoding, page 3-57
- Configuring Service Data Collaboration Support, page 3-59

Adding a Service

In the Services tab, you can add a completely new service, or a new service based upon an existing one.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Services** tab

Click **Add**.

The Select Service dialog box appears.

Step 3   To add a completely new service, click **New Service**.

–or–

To add a new service based on an existing one, click that service.

Step 4   Click **OK**.

The Add Service dialog box appears.

Related Topics

- About the Add Service and Edit Service dialog boxes, page 3-44

Editing a Service

In the Services tab, you can edit an existing service.

Procedure

Step 1   In the Administrator interface, on the sidebar, click **MCU** (if not already selected).

Step 2   Click the **Services** tab

Step 3   In the Services tab, double-click an existing service entry.

The **Edit Service** dialog box appears.

Related Topics

- About the Add Service and Edit Service dialog boxes, page 3-44

About the Add Service and Edit Service dialog boxes

You can configure or edit service settings in the Add Service or Edit Service dialog boxes. Figure 3-4 and Table 3-11 detail and list the elements of this dialog box.

Figure 3-4   *Add Service and Edit Service Dialog Box Elements*
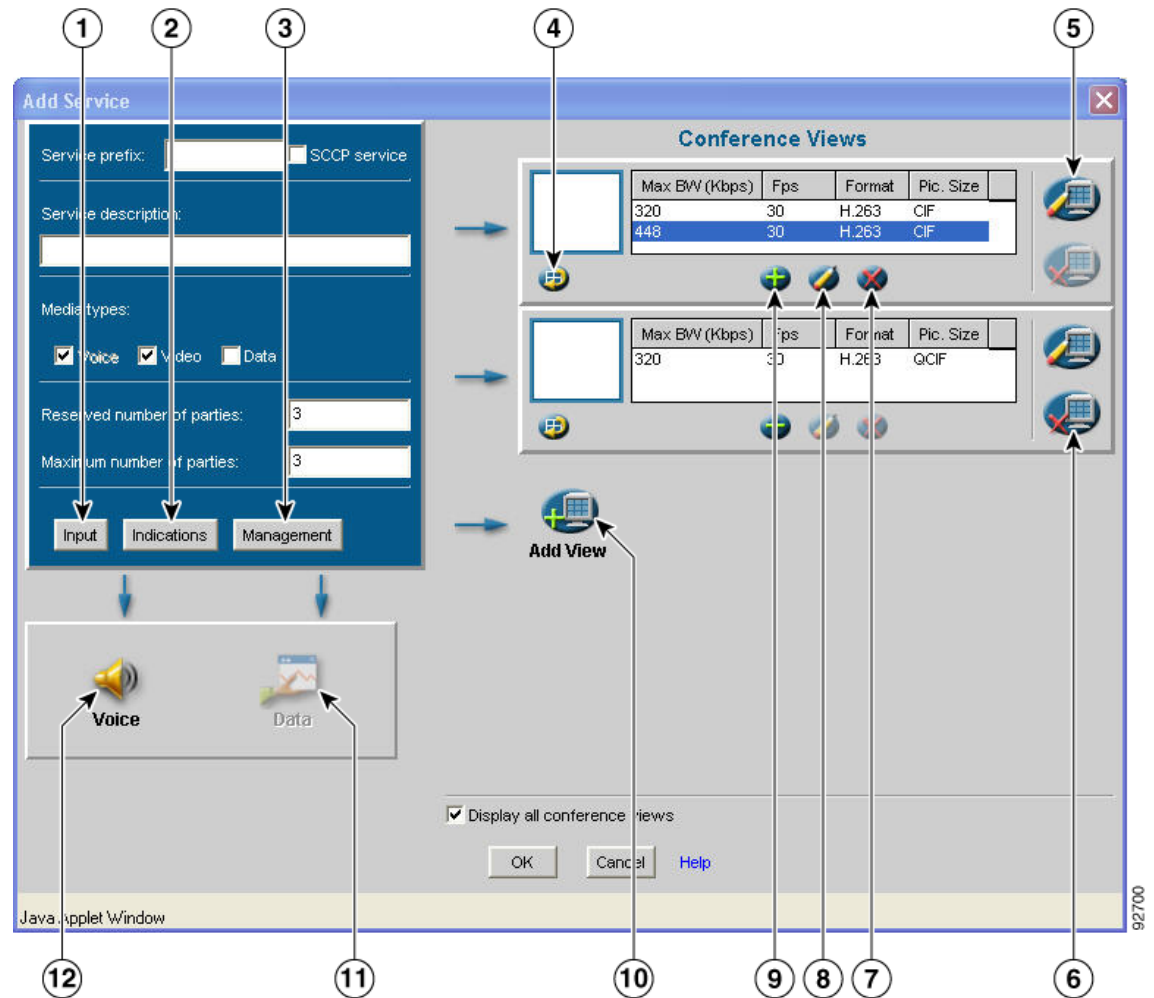
Table 3-11   *Add Service and Edit Service Dialog Box*

Number	Description
1	Input button
2	Indications button
3	Management button
4	Change Layout button
5	Edit View button
6	Delete Conference View button
7	Delete Video Scheme button
8	Edit Video Scheme button
9	Add Video Scheme button
10	Add View button

Table 3-11   *Add Service and Edit Service Dialog Box*

Number	Description
11	Data button
12	Voice button

Configuring Basic Service Settings

When adding or editing a service, in the Basic Settings section of the Add Service or Edit Service dialog box, you can configure general service settings such as prefix number, description, maximum participants, supported media, incoming video coding, audio indications, and conference management policies.

Before You Begin

Follow one of these procedures to add or edit a service:

- Adding a Service, page 3-43
- Editing a Service, page 3-44

Procedure

Step 1   In the **Service prefix** field, enter a prefix for the service.

Note   Make sure that the prefix number you set does not clash with existing network numbering assignments when the Cisco IPVC 35xx MCU incorporates the prefix into the conference ID you dial to start or join a conference.

Step 2   If this is an SCCP service, select the **SCCP service** check box.

Step 3   In the **Service description** field, enter a description of the type of conference view capabilities that the service features.

Step 4   In the Media types section, configure the media support available in the conference by selecting the appropriate check box:

- **Voice**—Always selected.
- **Video**—Selected by default. You can disable this option when setting up a voice-only service.
- **Data**—Select if the service supports T.120 data collaboration.

Note   Follow steps 5 and 6 for SCCP services only.

Step 5   In the **Reserved number of parties** field, enter the maximum number of reserved parties for participants attending a conference using the current service.

Step 6   In the **Maximum number of parties** field, enter a number representing the limit of the number of participants attending a conference using the current service that exceeds the reserved number specified in step #5. The additional number of participants beyond the reserved number of places is dependent on network resource availability when the conference is in progress.

Configuring Service Video Settings

In the Add Service or Edit Service dialog boxes, you can configure incoming video settings for a service. Service video settings update automatically according to conference view output settings.

⚠️
Caution   Changing these settings might cause the service to function incorrectly.

Before You Begin

Follow these procedures:

Procedure

Step 1   In the Add Service or Edit Service dialog box, click **Input**.

Step 2   Select the **Set Bit Rate Manually** check box to change video settings.

Step 3   In the **Max. Incoming Bit Rate (Kbps)** field, choose the maximum bit rate available for this service. This value represents the bit rate of the video stream only and does not include the bandwidth used by the voice stream. Bandwidth ranges from 65 Kbps to 2048 Kbps depending on the type of video processing support available and media types supported. This field lists the available video bandwidth rate and the combined audio and video rate for each value.

Step 4   In the **Video format** field, choose the incoming video format supported in conferences using this service:

- **H.261**
- **H.263**
- **H.264**

Step 5   To configure additional video coding techniques implemented by advanced H.263 encoders, follow these additional steps:

a.   Click the **H.263+** button.

The **Setting Incoming H.263+** dialog box appears.

b.   Select the desired techniques. For more information, see ITU-T RFC 2190.

⚠️
Caution   Terminals participating in a conference that do not support H.263+ features selected here cannot receive the conference video.

c.   Click **OK**.

Step 6   In the **Max. incoming picture size** field, choose the maximum incoming picture format supported in conferences using this service:

- **CIF**
- **QCIF**
- **4CIF**
- **SIF**
- **4SIF**

- **VGA**

- **SVGA**

- **XGA**

Step 7   In the **Max. incoming frame rate** field, choose the maximum incoming frame rate per second (Fps) supported in conferences using this service:

- **5**

- **7.5**

- **10**

- **15**

- **30**

Step 8   Click **OK**.

Configuring Service Indication Settings

In the Add Service or Edit Service dialog box, for a service, you can configure audio indications played to conference participants.

Before You Begin

Follow these procedures:

-

-

Procedure

Step 1   In the Add Service or Edit Service dialog box, click **Indications**.

The **Indications Settings** dialog box appears.

Step 2   Select the **First participant entry** check box if you want a message played to the first participant entering a conference, informing the participant that they are the first one to enter.

Step 3   Select the **Participant entry** check box if you want an audio indication played when any participant except the first participant enters a conference.

Step 4   Select the **Participant exit** check box if you want an audio indication played when any participant other than the last participant exits a conference.

Step 5   Select the **Conference termination warning** check box if you want a message played to participants 180 seconds before conference termination.

Step 6   Click **OK**.

Configuring Service Management Settings

In the Add Service or Edit Service dialog box, for a service, you can configure policies for password protection, invite authorizations, maximum sub-conferences, default chair password, Far End Camera Control (FECC), video quality, auto-reconnect, and auto-redial.

Before You Begin

Follow these procedures:

- Adding a Service, page 3-43 or Editing a Service, page 3-44
- Configuring Basic Service Settings, page 3-46

Procedure

Step 1   In the Add Service or Edit Service dialog box, click **Management**.

The **Management Settings** dialog box appears.

Step 2   Select the **Force conference password** check box to require a conference password when a user creates or enters a conference using this service. In ad hoc conferences, the first participant must set the password within the dialing string (using password delimiters). If the password is not set, the conference does not continue.

Step 3   Select the **Prompt invitees for password** check box to prompt both dial-in and dial-out participants to supply the password before entering the conference. If you do not select this option, only dial-in participants are required to enter the password.

> ✎
> **Note**   This option applies only for protected conferences.

Step 4   Select the **Conference manager invitees only** check box if you only want users with Chair Control-level access to invite participants into the conference.

Step 5   In the **Default chair password** field, enter a password used as the default password for taking Chair Control of conferences using this service.

Step 6   Select the **Support encryption** check box to enable Cisco IPVC 35xx MCU support for H.235 encryption for H.323 calls.

Step 7   If you did not perform step 6, skip to step 8. Otherwise, in the **Encryption mode** field, choose the required encryption mode:

- **Best effort**—This mode implements a "best effort" encryption algorithm. If an endpoint supports encryption, it connects in an encrypted way. If not, it connects without encryption.
- **Encryption required**—This mode only connects encrypted calls. Encryption is either AES 128 or DES 56. It does not allow non-encrypted calls to connect.
- **Strong encryption required**—This mode only allows AES 128 encrypted calls. It does not allow endpoints that do not support AES 128 to connect.

> ✎
> **Note**   An encrypted call uses double the resources of a regular call for all bandwidth rates. Cisco IPVC 35xx MCU capacity when encryption is supported is therefore half of regular Cisco IPVC 35xx MCU capacity.

Step 8   Select the **Enable Far End Camera Control** check box to enable support of Far End Camera Control (FECC) data for managing the camera of endpoints at other locations.

Step 9   Select the **Enable QualiVision** check box to enable the Cisco IPVC 35xx MCU packet loss compensation mechanisms for both transmitted and received packets for each service definition.

Step 10   Select the **Enable auto-reconnect** check box for the Cisco IPVC 35xx MCU to automatically call disconnected terminals to attempt a reconnection. The Cisco IPVC 35xx MCU attempts reconnection three times.

Step 11   Select the **Enable auto-redial** check box for the Cisco IPVC 35xx MCU to redial endpoints that fail to respond to conference invites. Follow these additional steps:

    a.   In the **Number of auto-redial** retries field, enter the number of redial attempts.

    b.   In the **Auto-redial interval (sec)** field, enter a number representing the number of seconds between each redial attempt.

Step 12   In the **Max Number of Sub-conferences** field, enter the maximum number of private audio sub-conferences that can be created during a conference using the current service.

Step 13   Click **OK**.

Configuring Conference Views

Conference views consist of layout and video scheme settings supported in the current service. You can configure conference view settings such as video output schemes, video switching behavior, and video processor support settings. You can create up to three video outputs per service in a combination of conference views and video schemes.

You can configure conference views in the Conference Views section of the Add Service or Edit Service dialog box. This section displays the currently configured conference views with the following information:

- Layout Frame—Displays the current video layout of the conference view.
- Max BW—Displays the maximum outgoing bandwidth for the video scheme.
- Fps—Displays the number of frames per second that the video scheme supports.
- Format—Displays the video coding format supported in the video scheme: H.261, H.263, or H.264.
- Pic. Size—Displays the image resolution supported in the conference view.

Before You Begin

Follow these procedures:

The following sections describe the components of conference view configuration:

Editing Video Layouts

The Cisco IPVC 35xx MCU has a wide range of video layouts depending on the type of video processing it supports and the protocol that is used, such as SCCP, H.323, and so on. Table 3-12 lists supported video layouts (*=supported).

Table 3-12   Supported Video Layouts

Layout	Cisco IPVC 35xx MCU	Rate Matching Module (RMM)	Enhanced Media Processor (EMP)
1 Participant	*	*	*
2 Participants			*
3 Participants			*
4 Participants[1]	*	*	*
5 Participants			*
6 Participants		*	*
7 Participants			*
8 Participants			*
9 Participants			*
10 Participants		*	*
13 Participants		*	*
16 Participants		*	*

1. For SCCP, the 4 participants layout requires an RMM or EMP.

Procedure

Step 1   In the Conference Views section of the Add Service or Edit Service dialog box, click **Change Layout**.

The Set Max Layout dialog box appears.

Step 2   Select the layout you want to use for this service.

Note   The 4 participants option is only available for an H.264 service if you select EMP in the Use Processor field of the Edit View dialog box. See the "Editing View Settings" section on page 3-53 for more information.

Step 3   Click **OK**.

Adding or Editing Video Schemes

You can set or edit video transcoding policies related to the layout in conference view video scheme settings. The range and functioning of configuration options depends upon the type of video processing support available to the Cisco IPVC 35xx MCU as follows:

- MCU—One video scheme supported
- MCU + RMM—Two video schemes supported in one conference view.
- MCU + EMP—Any combination of up to four video schemes and conference views.

Procedure

Step 1   In the Conference Views section of the Add Service or Edit Service dialog box, click the **Add Video Scheme Settings** button to add a new video scheme or select an existing on and click the **Edit Video Scheme Settings** button.

The Add Video Scheme or Edit Video Scheme dialog box appears.

Step 2   In the **Mode** field, choose how to define H.236 annexes used with the video scheme:

- **Basic**—Select any required annexes; no annexes are currently selected.
- **Natural Video (TF)**—Interfaced Fields (Annex W6.3.11) and CIF Additional Picture Memory are selected.
- **H263+(F)**—Advanced Prediction (Annex F) is selected.

Step 3   In the **Max. bit rate (Kbps)** field, choose the maximum output rate for the video stream.

> **Note**   The rate setting does not include the bandwidth that the voice stream uses. The voice stream rate is fixed according to the audio codec in use. For example, G.711 at 64 Kpbs, G.728 at 8 Kbps. Available rates can vary according to available video processing support.

Step 4   In the **Max. frame rate** field, choose the maximum outgoing frame rate per second (Fps) supported in conferences using this service.

> **Note**   Each output scheme has its own maximum frame rate. The Cisco IPVC 35xx MCU does not transmit video to an endpoint that does not support any of the available output schemes. Available rates can vary according to available video processing support.

Step 5   In the **Video format** field, choose the outgoing video format supported in conferences using this service.

> **Note**   Available rates can vary according to available video processing support.

Step 6   Click the **H.263**+ button to select additional video coding techniques implemented by advanced H.263 encoders. For more information about these video coding techniques, see ITU-T RFC 2190.

> **Caution**   Terminals participating in a conference that does not support H.263+ features that are selected in the service cannot receive the conference video

Step 7   In the **Picture size** field, choose the image resolution supported in the conference.

Step 8   In the **Video quality preference** field, scroll to select a preference for higher image quality or better motion.

Step 9   Select the **Allow dynamic scheme** check box if this video scheme operates in H.263+ (F) mode.

Step 10   In the **Min. Bit Rate (Kbps)** field, choose the minimum output rate in a range from 64 to 2048 Kbps. This is the bit rate of the video stream only and does not include the bandwidth used by the voice stream.

Step 11   Click **OK**.

Deleting Video Schemes

You can delete a video scheme from a conference view. However, each conference view must retain at least one video scheme.

Procedure

Step 1   In the Conference Views section of the Add Service or Edit Service dialog box, click the video scheme and then click the **Delete Video Scheme Settings** button.

Editing View Settings

In the Conference Views section of the Add Service or Edit Service dialog box, you can configure video layout settings, switching policies, and video scheme settings for a conference view.

Procedure

Step 1   In the Conference Views section of the Add Service or Edit Service dialog box, click the **Edit View** button.

The Edit View dialog box appears.

Step 2   The Max Layout field indicates the video layout displaying the maximum number of participants to which the conference view expands. To change the layout, follow these steps:

a.   Click the **Change** button.

The Set Max Layout dialog box appears.

b.   Select the layout you want to use for this service.

> **Note**   The 4 participants option is only available for an H.264 service if you select EMP in the Use Processor field (step #6).

c.   Click **OK**.

Step 3   The Initial Layout field indicates the video layout that appears when the conference begins. To change this layout, follow these steps:

a.   Click the **Change** button.

The Set Initial Layout dialog box appears.

b.   Choose a layout.

c.   Click **OK**.

Step 4 Select the **Use dynamic layout** check box if you want the participant video display to switch between layouts as participants join or leave the conference up to the maximum layout set in the Max Layout field. The precise order in which the layout changes is defined in the Dynamic Layouts section of the Settings tab. See the "Configuring Cisco IPVC 35xx MCU Dynamic Layouts" section on page 3-11 for more information.

Step 5 Select the **Display current speaker border** check box to display a highlight border around the video layout sub-frame of the current speaker.

> **Note**   You configure border color formats in the Themes section of the Settings tab. See the "Configuring Cisco IPVC 35xx MCU Themes" section on page 3-8 for more information.

Step 6 In the **Use Processor** field, choose the type of video processor support required for services using the current conference view. Service parameters are enabled or disabled in accordance with the type of capabilities supported by the selected video processor. The local MP performs audio processing. You can choose from one of the following options:

- **MP**—The MP component of the Cisco IPVC 35xx MCU performs video processing.

- **MP and RM**—The MP component of the Cisco IPVC 35xx MCU performs video processing with RMM support for additional layout options and rate matching support.

- **EMP**—An EMP unit performs video processing with advanced video processing options including a wide range of layouts, processing schemes, multiple views, and dual video support.

  > **Note**   The EMP option enables support for up to four CP layout for H.264 services.

- **Auto**—The conference view profile determines the type of video processor support required.

Step 7 The Video Scheme Policy field indicates the video scheme output handling policy. By default, the Cisco IPVC 35xx MCU sends video according to the maximum bit rate of the video scheme setting. You can change this configuration if all of the following conditions are met:

- You set the **Max Layout** field to a layout with multiple sub-frames (a layout of 2 x 2 or more).

- You set the **Use Processor** field to **MP and RM**.

- The two video schemes are configured for a conference view.

If these conditions are met, you can then choose one of the following options from the **Video Scheme Policy** field:

- **Maximum bit rate**—Video output bandwidth rate in conferences configured with this service layout is equal to the maximum bit rate specified when adding or editing a video scheme.

- **Symmetric to input**—Video output bandwidth rate in conferences configured with this service layout matches the incoming bandwidth rate from the conference participant.

Step 8 In the **Video Picture Size** field, you can choose the picture size format:

Step 9 In the **Display participant name** field, you can choose how to display the participant name in the video layout sub-frame:

> **Note**   This setting requires EMP support. You configure text format and background settings in the Themes section of the Settings tab.

- **Always**—The participant name always appears.

- **Never**—The participant name never appears.

- **On change**—The participant name always appears when the participant is first introduced or when the participant sub-frame location changes on the screen. The duration of the display of the participant name following the changes is defined in the Advanced section of the Settings tab. See the "Configuring Participant Name Display Duration" section on page 3-19 for more information.

Step 10   In the **Active theme** field, you can choose a theme:

> ✎
> **Note**   This setting requires EMP support.

- **Default**

- **Basic**

- **Blue Freeze**

- **Copper Autumn**

- **Charlie Chaplin**

- **Fresh Green**

> ✎
> **Note**   You can preview default themes and configure a custom theme in the Themes section of the Settings tab.

Step 11   In the **Adapt screen for** field, you can choose **TV monitor** to adapt the image size of the video to suit TV monitors since some monitors crop the image size of the video picture. Otherwise, you can select **Terminal display**. The default setting is **TV monitor**.

Step 12   Select the **Enable voice activate** check box if you want to set voice-activated video switching in the video display. Voice-activated video switching is a mode of operation where the Cisco IPVC 35xx MCU automatically switches the video image to display the active speaker in a conference. You can use this feature to access options for configuring the voice-activated (VA) method and zoom layout. If you perform this step, follow this additional step:

- **a.**   In the **Voice Activate Method** field, you can choose a method for displaying the active speaker in the video image of the conference:

    - **All see one**—All participants see the active speaker.

    - **See you see me**—In voice-activated (VA) mode, all participants see the participant that is talking the loudest. the participant current talking sees the previous speaker. In Continuous Presence (CP) mode, the Cisco IPVC 35xx MCU allocates one sub-frame to display the VA speaker. If the speaker already appears in another sub-frame, the image only moves to the allocated VA sub-frame if the VA frame size is larger than the current sub-frame.

    - **Zoom in**—The conference video image switches to the layout image specified in the Zoom in layout field when a speaker is active. This option is available when the maximum video layout is configured to a layout with more than one sub-frame and the **Use Processor** field is set to **EMP**. This option is useful for highlighting an active speaker in a conference view reserved for displaying participants who are usually inactive such as the audience in a lecture.

    - **Recent**—There is no allocated sub-frame for the VA speaker. This setting displays all of the most recent speakers. This option is available when the maximum video layout is configured to a layout with more than one sub-frame.

Step 13   From the **Zoom in layout** field, you can configure how the video layout appears when a speaker is active in a conference:

> **Note** This option is available only when the **Use Processor** field is set to **EMP** and the **Voice Activate Method** field is set to **Zoom in**.

    a. Click **Change**.

       The Set Zoom In Layout View dialog box appears.

    b. Choose the preferred layout to which the video switches in this mode.

> **Note** The range of available layouts depends on the service type and the video processing support available to the Cisco IPVC 35xx MCU. Cisco IPVC 35xx MCUs operating without video processing support allow a layout of up to four participant images. RMM support increases the range of layout combinations to a maximum of 16 images in a single display. EMP support includes a more advanced range of options.

    c. Click **OK**.

Step 14 Select the **Enable auto switch** check box to enable auto-switching in which participant images in the video layout periodically change to allow the display of other conference participants according to the interval set.

> **Note** You can enable or disable this setting during a conference.

Step 15 In the **Auto-switch interval** field, enter the interval between auto-switching operations when the participants images displayed in the layout change.

> **Note** You cannot reconfigure this setting during a conference

Step 16 You can configure current video coding output settings for the conference view. These settings include the number of video schemes supported, video bit rate, frames per second (Fps), video format, and picture size. You can configure video coding output settings in the following ways:

- To add a video scheme, click the **Add Video Scheme** button. See the "Adding or Editing Video Schemes" section on page 3-51 for more information.
- To edit a video scheme, click it in the Video Schemes Settings area and then click the **Edit** button. See the "Adding or Editing Video Schemes" section on page 3-51 for more information.
- To delete a video scheme, click it in the Video Scheme Settings area and then click **Delete**.

Step 17 Select the **Preserve this view when the conference is cascaded** check box to enable the operator of a slave conference (slave conferences occur in cascaded conferences) to switch the view for each participant in the slave conference so that the participant can see the view broadcasted by the master or the local view.

> **Note** This option is disabled if you have set more than one video scheme for the current view.

Step 18 Click **OK** to apply your settings.

Adding Additional Conference Views

For each service, in the Add Service or Edit Service dialog box, you can configure additional conference views provided that the Cisco IPVC 35xx MCU has EMP support. With multiple views, the speaker in a lecture can view participants while the audience views the speaker. In a conference with varying connection speeds, participants with high video capabilities and participants with low video capabilities can take part at the same time without one affecting the experience of one another.

✎
Note   If you add additional conference views, you cannot enable dual video.

Procedure

Step 1   In the Add Service or Edit Service dialog box, select the **Display all conference views** check box.

Step 2   Click the **Add View** button.

An additional conference views setting area appears.

Step 3   Configure the additional conference view. See the "Configuring Conference Views" section on page 3-50 for more information.

Deleting an Additional Conference View

If you configure an additional conference view, you can remove it in the Add Service or Edit Service dialog box.

Procedure

Step 1   In the Add Service or Edit Service dialog box, for the conference view you want to delete, click the **Delete Conference View** button.

Configuring Service Audio Transcoding

Transcoding between audio protocols enables the Cisco IPVC 35xx MCU to support communication between endpoints with codecs that are incompatible with each other. You configure service audio transcoding in the Add Service or Edit Service dialog box.

The Cisco IPVC 35xx MCU has processing capacity for audio transcoding up to 48 video calls. The Cisco IPVC 35xx MCU features optional transcoding using Digital Signal Processing (DSP) devices on the Cisco IPVC Audio Transcoding Module.

For a service, you can configure conference audio codec support and transcoding priorities. All Cisco IPVC 35xx MCU devices support the following audio codec:

• G.711 A/μ law—Toll quality at 64 Kbps (A-Law/mu-Law).

The following codes require the Cisco IPVC Audio Transcoding Module:

Note The Cisco IPVC Audio Transcoding Module is included with the Cisco IPVC 35xx MCU and Cisco IPVC 35xx MCU with EMP (E), but optional for the Cisco IPVC 3540 MCU module.

- G.722—High-quality audio at 64 Kbps.
- G.722.1—High quality audio at 24 Kbps or 32 Kbps using a digital sampling rate ranging from 50 Hz up to 7 kHz.
- G.723.1—Voice quality audio at 5.3 Kbps or 6.4 Kbps.
- G.728—Near toll quality audio at 16 Kbps.
- G.729A—Audio at 8 Kbps.

Procedure

Step 1 In the Add Service or Edit Service dialog box, click the **Voice** button.

The Audio Settings dialog box appears.

Step 2 The Transcoder Priority field displays the choice of codecs that you prefer for audio transcoding. The codes are listed in declining order of preference with the most preferred codec listed first. Setting these priorities notifies the Cisco IPVC 35xx MCU and remote endpoints of your preferred audio codecs. This is useful when more than one codec is supported by both sides. To change these priorities, follow these steps:

    a. Click **Change**.

    The Transcoder Priority Settings dialog box appears, listing supported audio codecs in the left-side section and the list of codec priorities in the right-side section.

    b. To add a transcoder to the Priority Order field, click it and then click **Add**. To remove a transcoder from the Priority Order field, click it and then click **Remove**.

    c. To move a transcoder up the priority list, click it and then click the **Up** button. To move a transcoder down the priority list, click it and then click the **Down** button.

    d. Click **OK**.

Step 3 In the **Mixer rank** field, enter the maximum number of speakers in a conference who can be heard at the same time. The value you enter is the number of loudest speakers for whom the audio stream is mixed and sent to all conference participants. For example, if you enter 4, the Cisco IPVC 35xx MCU mixes the audio stream of the four loudest speakers in the conference.

Step 4 In the **Packet size** field, enter the minimum audio packet size.

Step 5 In the **New speaker interval (millisec)** field, enter the interval (in milliseconds) before the voice-activated video-switching mechanism displays a new active speaker in the video image. The default setting is 3000 milliseconds.

Step 6 Select the **Conference participants initially muted** check box to have the Cisco IPVC 35xx MCU initially mute all participants joining the conference. Once the conference begins, the conference Chair Control can unmute selected participants. This is useful for lectures.

Step 7 If you performed step 6, you can select the **Do not mute first conference participant** check box to have the Cisco IPVC 35xx MCU mute all conference participants except the participant that joined the conference first.

Step 8 Click **OK**.

Configuring Service Data Collaboration Support

For a service, you can configure settings for incoming T.120 data collaboration settings in the Add Service or Edit Service dialog box.

> **Note** Support for T.120 data collaboration is through the Cisco IPVC 3540 Application Server (AS) Module for Data Collaboration Server (DCS) only.

Procedure

Step 1 In the Media types section of Add Service or Edit Service dialog box, select the **Data** check box.

Step 2 Click **Data**.

The Data Settings dialog box appears.

Step 3 In the **Reserved number of T.120 ports**, enter the number of T.120 ports reserved for use in a conference that uses this service on the data collaboration server that supports this Cisco IPVC 35xx MCU.

Step 4 Select the **Allow access to T.120 data conference via MCU web** check box to enable T.120 endpoints not directly involved in a video conference to participate in a data collaboration session with the other video conference participants. If you do not enable this setting, you can only create data sessions from endpoints participating in the corresponding video conference.

Step 5 Click **OK**.

Enabling the Dual Video Feature

The Cisco IPVC 35xx MCU can produce multiple output for display on video conferencing room systems and endpoints supporting two screens using the H.239 standard of TANDBERG DuoVideo.

The dual video feature produces a participant video image and a presentation view in the same conference. The video image of the conference participants appears on one screen and the presentation appears on the other screen.

You can configure a service to support conferences producing output to room systems with two monitors. Thus, a presentation appears on one monitor while conference video images appear on the other monitor.

> **Note** You cannot enable this setting if you configure an additional conference view for this service.

Procedure

Step 1 In the Conference Views section of the Add Service or Edit Service dialog box, select the **Enable Dual Video** check box.

Deleting Services

In the Services tab, you can delete configured services.

Procedure

Step 1   In the **Services** tab, click a service.

Step 2   Click **Delete**.

Viewing the Event Log

The Event Log tab displays a list of reported alarm events. These events are configured in the Alert Indications section of the Settings tab.

The Event Log tab displays the following information:

- Event ID—Displays the identifier for the specified alarm event.
- Time—Displays the date and time when the reported event occurred.
- Severity—Displays the severity of the reported event.
- Message—Displays the error message used to report the event

About Cisco IPVC 35xx MCU Resource Allocations

This section details call capacities supported by the Cisco IPVC 35xx MCU with video processing support and Rate Matching Module (RMM) capabilities. This section describes the following topics:

About Cisco IPVC 35xx MCU Call Capacities

Table 3-13 lists the maximum call capacities at different audio and video bandwidth rates on Cisco IPVC 35xx MCUs with EMP video processing support.

The call capacities are supported in the following scenarios:

- Calls in voice-activated (VA) mode or full screen mode.
- Continuous Presence (CP) calls with EMP video processing support.

Table 3-13   Cisco IPVC 35xx MCU Call capacities

Call Type	Bandwidth		Maximum Calls for Cisco IPVC 35xx MCU Type			
	Call Rate	B Channels	3540 MCU-MC10A	3540 MCU-MC06A	3540 MCU-MC03A	3511 MCU
A[1]	64	1	150	90	45	26
B[2]	Voice Transcoding		15	48[3]	30	15
C	128	2	100	60	30	15

Table 3-13   Cisco IPVC 35xx MCU Call capacities

Call Type	Bandwidth			Maximum Calls for Cisco IPVC 35xx MCU Type			
	Call Rate	B Channels		3540 MCU-MC10A	3540 MCU-MC06A	3540 MCU-MC03A	3511 MCU
D	192	3		100	60	30	15
E	256	4		80	48	24	12
F	320	5		74	48	24	12
G	384	6		70	48	24	12
H	512	8		60	48	24	12
I	640	10		51	48	24	12
J	768	12		48	48[4]	24	12
K	1024	16		41	38	18	8
L	1344	Res T1		34	28	14	7
M	1472	Full T1		28	24	12	6
N	1536	1.5M		26	22	11	6
O	1984	31(E1)		22	16	8	4
P	2048	2M		22	16	8	4

1. Voice Only calls.

2. The maximum number of voice transcoded calls for each Cisco IPVC 35xx MCU. Subtract this value from the total at any given call rate.

3. Requires EMP support to achieve the maximum number of audio transcoded calls for calls at this rate. Otherwise, the maximum is 30.

4. Requires EMP support to achieve the maximum number of conferences supporting calls at this rate.

About RMM Call Capacities

Table 3-14 lists the maximum call capacities at different audio and video bandwidth rates on Cisco IPVC 35xx MCUs with Rate Matching Module (RMM) video processing support.

The call capacities are supported in the following scenarios:

- Asymmetric CP4 calls.

- All CP modes with RMM support.

Table 3-14   Call Capacities on MP Only Units or with RMM Support

Call Type	Bandwidth			Maximum Calls for Cisco IPVC 35xx MCU Type			
	Video	Video and Voice (64K)	B Channels	3540 MCU-10A	3540 MCU-06A	3540 MCU-03A	MCU 3511
U	110	174	2[1]	66	40	20	10
V	128	192	3	64	39	19	9
W	170	234	3[1.]	61	37	18	9

Table 3-14   Call Capacities on MP Only Units or with RMM Support

Call Type	Bandwidth			Maximum Calls for Cisco IPVC 35xx MCU Type			
	Video	Video and Voice (64K)	B Channels	3540 MCU-10A	3540 MCU-06A	3540 MCU-03A	MCU 3511
X	192	256	4	59	37	18	9
Y	220	284	4[1.]	57	36	18	9
Z	320	384	6	50	32	16	8

1. The number of B Channels is calculated to include the maximum video bandwidth.

About RMM Conference Capacities

Table 3-15 shows RMM conference capacities according to supported CP layouts at different call rate values.

Table 3-15   RMM Conference Capabilities

Conference Format	Maximum conferences supported by video call rate (Kbps)[1]			
	Asymmetric		Symmetric	
	In 105 / Out 440 [2]	In 320 / Out 1280	In 105 / Out 105	In 320 / Out 320
CP4[3]	No limit	No limit	6	4
3+4[4]	8	5	2.5[5]	2
2+8	4	2.5	2	1.5[5.]
1+12	2.5	1.5	1.5	1
CP16	2	1	1	0.7[6]

1. All modes are 15 fps, QCIF in, CIF out.

2. The "In" value represents the bit rate of the incoming video stream. The "Out" value represents the bit rate of the outgoing video stream.

3. CP = Continuous Presence.

4. Figures refer to the number of large participant images on the screen plus the number of small participant images for the specified conference format.

5. A conference value of 2.5 means that two conferences can be supported when one RMM is present in the system, and five conferences can be supported when two RMM modules are present. Similarly, a value of 1.5 means that one conference can be supported when one RMM is present in the system, and three conferences can be supported when two RMM modules are present.

6. A conference value of 0.7 means that no conferences can be supported when only one RMM is present in the system, but one conference can be supported when two RMM modules are present.

Configuring the Cisco IPVC 35xx MCU to Use Cisco MeetingPlace

You can use a Cisco IPVC 35xx MCU to provide video content for Cisco MeetingPlace conferences in H.323 environments. To provide video content in Cisco MeetingPlace conferences, you must configure your Cisco MeetingPlace components and your Cisco IPVC 35xx MCU.

See the *Administrator's Guide* for Cisco MeetingPlace Video Integration Release 5.3 for information about configuring your Cisco MeetingPlace components.

To configure the Cisco IPVC 35xx MCU to use Cisco MeetingPlace, follow the steps outlined in these topics:

> **Note** You cannot stack embedded Cisco IPVC 35xx MCU media processors to use with Cisco MeetingPlace.

Verifying that Video Endpoints Can Connect to the Cisco IPVC 35xx MCU

Endpoints must be able to join video conferences on the Cisco IPVC 35xx MCU before Cisco MeetingPlace Video Integration can run.

If you have questions about routing calls through the gatekeeper and you use a Cisco IOS H.323 Gatekeeper, see the *Cisco IOS H.323 Configuration Guide.*

Creating a Cisco IPVC 35xx MCU User for Cisco MeetingPlace

You can create a user name and password that Cisco MeetingPlace Video Integration uses to log in to the Cisco IPVC 35xx MCU. After you create a Cisco IPVC 35xx MCU user name for Cisco MeetingPlace, you must make the user name available to the Cisco MeetingPlace video server through the Cisco MeetingPlace video server installation utility.

For information about installing, upgrading, and configuring the Cisco MeetingPlace video server, see the *Administrator's Guide* for Cisco MeetingPlace Video Integration Release 5.3.

Procedure

Step 1   Log in to the Administrator interface of the Cisco IPVC 35xx MCU that you want Cisco MeetingPlace to use.

Step 2   On the sidebar, click **Board**.

Step 3   Click the **Users** tab.

Step 4   Click the **Add** button.

The Add User dialog box appears.

Step 5   In the **User name** field, enter the name that you want the Cisco MeetingPlace Web Conferencing server to use to log in to theCisco IPVC 35xx MCU.

Step 6   In the **Access level** field, choose **Administrato**r or **Operator**.

Step 7   In the **Password** field, enter the password that you want this user to have.

Step 8   In the **Confirm Password** field, re-enter the password that you entered in step 7.

Step 9   To disable the ability of this user to telnet into the Cisco IPVC 35xx MCU, unselect **Enable for Telnet / FTP**.

Step 10   Click **Upload**.

Setting Cisco IPVC 35xx MCU Parameters Required to Support Cisco MeetingPlace

To use your Cisco IPVC 35xx MCU with Cisco MeetingPlace, you must configure certain Cisco IPVC 35xx MCU parameters to provide video for Cisco MeetingPlace conferences.

Procedure

Step 1   Log in to the Administrator interface of the Cisco IPVC 35xx MCU that you want the Cisco MeetingPlace server to use.

Step 2   On the sidebar, click **MCU**.

Step 3   Click the **Settings** tab and then click the **Conference Mgmt** button.

Step 4   Set the following parameters in the Conference Mgmt page:

   a.   In the **External conference authorization policy** field, choose **Authorize**.

   b.   In the **Allow conference creation using** field, choose **Scheduler, Web, Control API and dial-in**.

   c.   In the **Allow conference joining using** field, choose **Invite and dial-in**.

   d.   In the **Dial-in conference terminates when** field, choose **Last participant leaves**.

Step 5   Click **Advanced**.

Step 6   We recommend that you select the **Disconnect participants on communications (ICMP) failure** check box and choose **Audio failure** from the **Disconnect on** field.

Step 7   Click **Upload**.

Setting the Audio Indication Interval (Optional)

If video participants join a conference that has not yet started, they must wait in the waiting room. To play an announcement while participants wait, set the following parameter:

Procedure

Step 1   On the sidebar, click **MCU**.

Step 2   Click the **Settings** tab.

Step 3   Click **Advanced**.

Step 4   Click **Commands**.

The Advanced Commands dialog box appears.

Step 5   In the Advanced Commands dialog box, do the following:

a.   In the **Available commands** field, click **First audio announcement interval (Msec).**

Your selection appears in the Command field.

b.   In the **Parameter** field, enter the value in milliseconds that you want Cisco MeetingPlace to wait before announcing to participants that they are in the waiting room and that the conference has not formally started. We recommend entering 1500 to establish an interval of 15 seconds.

c.   Click **Send**, then click **Close**.

Creating a Service for Cisco MeetingPlace

You must create a Cisco IPVC 35xx MCU service for Cisco MeetingPlace. Before you create a service in the Cisco IPVC 35xx MCU make sure that the media processor (MP) that the Cisco IPVC 35xx MCU uses supports Cisco MeetingPlace.

Table 3-16 lists information about which Cisco IPVC 35xx MCU media processors support Cisco MeetingPlace releases.

Table 3-16   Media Processors That Support Video in Cisco MeetingPlace, Release 5.3

Cisco IPVC Media Processor	Software Supporting Cisco MeetingPlace
Local Cisco IPVC 35xx MCU media processor	Release 3.5.24 or later releases
Enhanced Media Processor (EMP)	Release 2.0.11 or later releases
Rate Matching Module (RMM)	Does not support Cisco MeetingPlace
Data Collaboration Server (DCS)	Does not support Cisco MeetingPlace

To create a service for Cisco MeetingPlace, follow one of these procedures:

- Using Pre-configured Service Templates, page 3-65
- Creating a Custom Service for Cisco MeetingPlace, page 3-66

Using Pre-configured Service Templates

Cisco IPVC 35xx MCU Releases 3.5.24 and later include three pre-configured services designed for Cisco MeetingPlace.

⚠

Caution   The Cisco MeetingPlace service prefixes appear automatically in the Services tab of the Administrator interface page for new Cisco IPVC 35xx MCUs. However, these services do not appear when you upgrade your Cisco IPVC 35xx MCU to Release 3.5.24 or Release 3.5.33. To display these services, you must use the restore factory defaults option. In doing so, you lose your current configuration.

Procedure

Step 1   Run the Cisco IPVC 35xx MCU installer.

Step 2   At the first install window, click **Customize**.

Step 3   Select the **MCU Config File** check box.

Step 4   Continue with the installation.

Step 5   After installation, log in to the Administrator interface.

Step 6   On the sidebar, click **MCU**.

Step 7   Click the **Services** tab.

Step 8   In the **Services** tab, choose the appropriate template for your needs. The Voice Activated view enables the View Active Speaker feature for participants, while the Continuous Presence view enables the View Multiple People for participants. Table 3-17 lists the settings are available to participants in the web-conferencing meeting room:

Table 3-17   *Cisco MeetingPlace Service Templates*

Service Prefix	Supported Views	Supported Endpoints	Processors Required	Format	Allow Dynamic Scheme
887	Voice Activated and Continuous Presence	H.323	MP	H.261	Unselected
888	Voice Activated	SCCP, H.323	MP	H.263	Selected
889	Voice Activated and Continuous Presence	SCCP, H.323	MP and EMP	H.263	Selected for both views

Creating a Custom Service for Cisco MeetingPlace

To create a custom Cisco IPVC 35xx MCU service for Cisco MeetingPlace, perform the following tasks:

- Setting the Core Service Parameters, page 3-66
- Setting Audio Indications, page 3-68
- Making Sure that a Conference Password Is Not Required, page 3-68
- Setting Conference View Parameters, page 3-68
- Creating Two Separate Views, page 3-70
- Setting Video Schemes Parameters, page 3-71

Setting the Core Service Parameters

When creating a service for Cisco MeetingPlace, you must configure certain core parameters in the Settings tab of the Administrator interface.

Procedure

Step 1 On the sidebar, click **MCU**.

Step 2 Click the **Services** tab.

Step 3 Click the **Add** button.

The Select Service dialog box appears.

Step 4 Make sure that **New service** is selected and click **OK**.

The Add Service dialog box appears.

Step 5 In the **Service prefix** field, enter the value that you want to use for the Cisco MeetingPlace service.

Step 6 Make sure that the **SCCP Service** check box is unselected.

> **Note** Users of SCCP endpoints can still attend Cisco MeetingPlace conferences.

Step 7 In the **Service description** field, enter the description for this service that you want to appear in the Create Conference window.

Step 8 In the **Media types** section, select the **Video** check box.

> **Note** Cisco MeetingPlace provides data collaboration in conferences. Disable data collaboration in the Cisco IPVC 35xx MCU if it is currently enabled. See the "Configuring Service Data Collaboration Support" section on page 3-59 for more information.

Step 9 Configure the number of ports that you want the Cisco IPVC 35xx MCU to reserve for each conference as follows:

    a. In the **Reserved number of parties** field, enter **2**.

> **Note** One of these ports is reserved for the Cisco MeetingPlace server.

    b. In the **Maximum number of parties** field, enter the total number of Cisco IPVC 35xx MCU ports that are available for conferences.

Tips

For step 9, you can ascertain the maximum number of ports this service can support by entering 200 in the Maximum number of parties field and choosing **OK** at the bottom of the page. The error message that appears indicates the maximum number of ports the current configuration supports based on the video bandwidth value specified in the Conference Views section.

Setting Audio Indications

When creating a service for Cisco MeetingPlace, we recommend that you enable all audio-indication parameters in the Add Service dialog box.

Procedure

Step 1   In the Add Service dialog box, click **Indications**.

The Indications Settings dialog box appears.

Step 2   Make sure that all parameters are selected.

Step 3   Click **OK**.

Making Sure that a Conference Password Is Not Required

When creating a service for Cisco MeetingPlace, make sure that the service does not require a conference password by verifying this setting in the Management Settings dialog box.

Procedure

Step 1   In the Add Service dialog box, click the **Management** button.

The Management Settings dialog box appears.

Step 2   Make sure that the **Force conference password** and **Prompt invitees for password** check boxes are unselected.

Step 3   Click **OK**.

The Add Services dialog box appears.

Setting Conference View Parameters

When you configure view parameters for a service to be used with Cisco MeetingPlace, use the Cisco MeetingPlace service template as a model. A Voice Activated view enables the View Active Speaker feature for participants, while a Continuous Presence view enables the View Multiple People feature for participants.

Because SCCP endpoints require the H.263 format, you need to configure special view settings in the Add Service dialog box. If your users will attend through SCCP endpoints and your Cisco IPVC 35xx MCU only has an MP card, you can only the Voice Activated view. In this case, all participants can only use the View Active Speaker option available in the Cisco MeetingPlace meeting room. They cannot view multiple people simultaneously.

You can set these conference view parameters in the Add Service dialog box.

Procedure

✐
Note   One Voice Activated, 1-participant layout is required. A Continuous Presence view is optional, if your hardware supports it.

Step 1 In the Conference Views section of the Add Service dialog box, click the **Edit View** button.

The Edit View dialog box appears.

Step 2 In the **Use Processor** field, choose the type of media processor that you want this service to use.

> ✎
> **Note**   The **MP and RM** option does not support Cisco MeetingPlace.

- Choose **MP** for the service to only use the local media processor to process video conference calls.
- Choose **EMP** for the service to use the Enhanced Media Processor (EMP) with the Cisco IPVC 35xx MCU to process video conference calls.
- Choose **Auto** for the Cisco IPVC 35xx MCU to choose the media processor that it uses to process a specific video conference.

> ✎
> **Note**   See *Cisco IP/VC 3511 MCU and Cisco IP/VC 3540 MCU Module Administrator Guide*, Version 3.2 for information about registering a media processor with the Cisco IPVC 35xx MCU.

Step 3 In the **Video Picture Size** field, choose the video format that most endpoints use.

Step 4 To enable the Cisco IPVC 35xx MCU to switch the video to the speaker who is speaking the loudest, select the **Enable voice activate** check box.

Step 5 In the **Voice Activate Method** field, we recommend that you click **All see one** to have all participants see the current speaker.

Step 6 To disable automatic switching of non-speaking participants, deselect the **Enable auto-switch** check box.

For SCCP endpoints, perform the following additional steps. Otherwise, skip to step 9.

Step 7 Set the initial layout to 1 participant:

   a. In the **Initial Layout** field, click the **Change** button.

   The Set Initial Layout dialog box appears.

   b. Make sure that **1 participant** is selected.

   c. Click **OK**.

Step 8 Set the max layout to 1 participant:

   a. In the **Max Layout** field, click the **Change** button.

   The Max Layout dialog box appears.

   b. Make sure that **1 participant** is selected.

   c. Click **OK**.

Step 9 Set the Max Processor field to **MP**.

Step 10 Set the video scheme format to H.263:

   a. In the Video Schemes Setting section, click the video scheme and then click the **Edit** button.

   The **Edit Video Scheme** dialog box appears.

   b. In the **Video format** field, choose **H.263**.

      c. Click **OK**.

Step 11 Click **OK** to save these conference view parameters.

Creating Two Separate Views

When creating a service for Cisco MeetingPlace, if your users will attend through SCCP endpoints and you have both an MP card and an EMP card, create two views in the service. This way, participants can use both the View Active Speaker and the View Multiple People features that are available in the Cisco MeetingPlace web-conferencing meeting room.The View Active Speaker feature corresponds to the Voice Activated view, and the View Multiple People feature corresponds to the Continuous Presence view. You can create two views for a service in the Add Service dialog box.

Procedure

Step 1 In the Add Service dialog box, click the **Edit View** button.

The Edit View dialog box appears.

Step 2 Set the initial layout to the desired multiple participant layout:

      a. In the **Initial Layout** field, click **Change**.

      The Set Initial Layout dialog box appears.

      b. Click the desired layout.

      c. Click **OK**.

Step 3 Set the max layout to the desired multiple participant layout:

      a. In the **Max Layout** field, click **Change**.

      The Set Max Layout dialog box appears.

      b. Click the desired layout.

      c. Click **OK**.

Step 4 In the **Use Processor** field, choose **EMP**.

Step 5 Set the video scheme format to H.263:

      a. In the Video Schemes Setting section, click the video scheme and then click the **Edit** button.

      b. The **Edit Video Scheme** dialog box appears.

      c. In the **Video format** field, choose **H.263**.

      d. Click **OK**.

Step 6 Set other parameters as you want.

Step 7 Click **OK**.

Step 8 Select the **Display all conference views** check box.

Step 9 Click **Add View**.

Now set parameters for the second view.

Step 10 For the second view, click the **Edit View** button.

Step 11 Repeat step 2 but set the initial layout to **1 participant**.

Step 12   Repeat step 3 but set the max layout to **1 participant**.

Step 13   Repeat step 4 but choose **MP**

Step 14   Repeat step 5.

Step 15   Set other parameters as you want

Step 16   Click **OK**.

Setting Video Schemes Parameters

When creating a service for Cisco MeetingPlace, you must configure certain video scheme parameters in the Edit Video Scheme dialog box.

Step 1   In the Conference Views section, click the **Edit View** button.

Step 2   In the Video Schemes Settings section, select the video scheme settings profile and click the **Edit** button.

The Edit Video Scheme dialog box appears.

Step 3   In the **Max bit rate (Kbps)** field, choose the maximum video bandwidth that you want this service to support. This number must be less than or equal to the bandwidth settings in Cisco MeetingPlace (and in Cisco CallManager if your network uses Cisco CallManager.)

Note   Endpoints that are not capable of supporting this bandwidth receive only the conference audio unless dynamic scheme is enabled.

Step 4   Select the **Allow dynamic scheme** check box to enable the Cisco IPVC 35xx MCU to switch the conference video bandwidth to a lower value when a less capable endpoint joins the conference.

Step 5   In the **Min bit rate (Kbps)** field, choose the lowest bandwidth that you want this parameter to support.

Step 6   Click **OK**.

Step 7   Click **OK**.

Saving Configuration Settings

You can save Cisco IPVC 35xx MCU configuration settings by exporting the configuration file to a storage device on your network. You can use the file you save to restore the settings on the current Cisco IPVC 35xx MCU or to configure a similar Cisco IPVC 35xx MCU. For example, you can use a Cisco IPVC 3511 MCU file that you save to configure another Cisco IPVC 3511 MCU.

Note   This operation does not save the user access level profiles that authorize users to access the Administrator or Conference Control interfaces.

Procedure

Step 1   Launch the Administrator interface for the Cisco IPVC 35xx MCU for which you want to save the configuration settings.

Step 2   Review each of the configuration pages to ensure that these are the configuration settings you want to save.

Step 3   Make sure the **MCU** button is selected.

Step 4   On the toolbar, click **Export**.

The File Download dialog box appears.

Step 5   Choose the **Save this file to disk** radio button.

Step 6   Click **OK**.

The Save as dialog box appears.

Step 7   In the **Save in** field, locate the directory in which you want to save the file.

The default file name is mcucfg.ini. You can change the file name to provide information about the contents for reference. Do not alter the file extension.

Step 8   Click **Save**.

The Download complete dialog box appears.

Step 9   Click **Close**.

Restoring the Configuration Settings

You can import an Cisco IPVC 35xx MCU file that you saved to a similar Cisco IPVC 35xx MCU. For example, you can use an Cisco IPVC 3511 MCU configuration file that you save to restore the configuration parameters on the same device or to configure another Cisco IPVC 3511 MCU. Similarly, you can use the configuration file that you saved for a Cisco IPVC 3540 MCU to restore the configuration on the same device or to configure another Cisco IPVC 3540 MCU.

Procedure

Step 1   Launch the Administrator interface for the Cisco IPVC 35xx MCU that you want to configure.

Step 2   Make sure the **MCU** button is selected.

Step 3   On the toolbar, click **Import**.

The Import a Configuration File dialog box appears.

Step 4   In the **File name** field, enter the path to the configuration file that you want to import.

Note   The file must have an .ini extension.

Step 5   Click **Import**.

> **Note**   You can verify the settings by clicking **MCU** or **Board** on the sidebar. However, to save the settings in either section, you must click **Upload** to save them before viewing the next section.

Step 6   On the toolbar, click **Upload**.

> **Note**   Uploading the file resets the device.

Using the Cisco IPVC 35xx MCU

This chapter describes the following topics:

About Using the Cisco IPVC 35xx MCU

You can participate in video conferences hosted on the Cisco IPVC 35xx MCU from any phone, terminal, or endpoint on any type of network to which the Cisco IPVC 35xx MCU connects. The Cisco IPVC 35xx MCU can accept calls from H.323, Skinny Client Control Protocol (SCCP), and Session Initiation Protocol (SIP) endpoints, and with Cisco IPVC video gateway support, from phones and terminals on H.320 and PSTN networks in the same conference.

You can participate in a conference by dialing from a phone, from an endpoint application, or by using the Cisco IPVC 35xx MCU Conference Control interface.

With appropriate access rights, you can also create conferences, invite other participants and conferences, and use an extensive range of conference control features for enhancing the video conferencing experience.

Making an Ad Hoc Conference Call

All users can create or join an ad hoc (also called dial in) conference simply by dialing the conference number. Users can invite single or multiple participants in the same operation.

Users can initiate multipoint conferences that run unattended and do not require advance configuration. Users simply dial a number and the Cisco IPVC 35xx MCU automatically sets up the conference. Anyone else who dials that number can join the conference at any time, provided that network resources are available. All that the user requires is a suitable service number—that an Administrator supplies—to combine with a unique number for the conference. A common practice is to use the telephone extension number of the conference creator as the unique number.

About Cisco IPVC 35xx MCU Dialing Conventions

This section describes the dialing conventions that relate to tasks users perform in ad hoc conferences:

- Starting or joining a conference with an H.323 endpoint. See the "About Starting or Joining an Ad Hoc Conference with H.323 Endpoints" section on page 4-2 for more information.
- Inviting participants with an H.323 endpoint. See the "About Inviting H.323 Endpoints" section on page 4-2 for more information.
- Working with SIP endpoints. See the "About Dialing Conventions with SIP Endpoints" section on page 4-3 for more information.
- Working with IP endpoints. See the "Using Dialing Conventions with IP Endpoints" section on page 4-4 for more information.

About Starting or Joining an Ad Hoc Conference with H.323 Endpoints

To start or join an ad hoc conference with H.323 endpoints, you dial in using the conference ID number. The conference ID number is composed of a service prefix number that indicates the conference call type and capabilities and a unique number that identifies the conference:

<Service prefix> + <Unique number>

A conference ID can consist of any combination of the characters 1-9, *, and #. It can be up to 256 characters in length.

For example, you can dial:

601234

Whereas:

- 60 is the service prefix.
- 1234 is the unique conference number.

As soon as the Cisco IPVC 35xx MCU accepts the call, you are connected to the existing conference, or the Cisco IPVC 35xx MCU creates a new conference with this conference identifier.

Note   Users should contact their Cisco IPVC 35xx MCU Administrator for a list of available conference services and service prefix numbers.

About Inviting H.323 Endpoints

With an H.323 endpoint, you can create or join an ad hoc conference and invite single or multiple participants in the same operation using the invite sign (**). You use the invite sign to separate the called numbers in the dialed string:

<conference ID number> + <**> + <invited participant number>

For example, you can dial:

601234**5678

Whereas:

- 601234 is the conference ID number.

- ** is the invite sign.

- 5678 is the invited participant number.

Note   You can invite multiple participants in one action by using the invite sign to separate each individual participant number.

About Dialing Conventions with SIP Endpoints

On Cisco IPVC 35xx MCUs supporting SIP protocol call signalling, you can dial to the Cisco IPVC 35xx MCU from SIP endpoints. You can also invite SIP endpoints to ad hoc conferences on the Cisco IPVC 35xx MCU when each is registered with a SIP proxy server on the IP network. The Cisco IPVC 35xx MCU domain name should be registered on a Domain Name System (DNS) or Microsoft Real Time Communications (RTC) server.

The following topics describe dialing conventions with SIP endpoints:

- About Starting or Joining Ad Hoc Conferences with SIP Endpoints, page 4-3

- About Inviting SIP Endpoints, page 4-3

- Dialing into the Cisco IPVC 35xx MCU Configured as a UAC from Another UAC, page 4-4

- Dialing into the Cisco IPVC 35xx MCU Configured as a Separate SIP Domain from a UAC, page 4-4

About Starting or Joining Ad Hoc Conferences with SIP Endpoints

When starting or joining an ad hoc conference, the dialed string should contain the conference ID number and the Cisco IPVC 35xx MCU domain name:

<conference ID number> @ <mcu.domain.com>

For example, you can dial:

601234@mcu.domain name

Whereas:

- 601234 is the conference ID number.

- @mcu.domain.com is the Cisco IPVC 35xx MCU domain.

About Inviting SIP Endpoints

You can dial from a SIP endpoint and invite an H.323 or SIP endpoint when the inviting SIP endpoint is registered in the Cisco IPVC 35xx MCU domain. The Cisco IPVC 35xx MCU adds the default domain to the dialed string when a user name is dialed without a domain:

<conference ID number> + <**> + <invited SIP endpoint>

For example, you can dial:

601234**john@mcu.domain.com

Whereas:

- 601234 is the conference ID number.
- ** is the invite sign.
- john@mcu.domain.com is the invited participant and domain.

Dialing into the Cisco IPVC 35xx MCU Configured as a UAC from Another UAC

Administrators can configure a Cisco IPVC 35xx MCU as a SIP-complaint endpoint called a User Agent Client (UAC). Users can start or join an ad hoc conference by dialing into this Cisco IPVC 35xx MCU from another UAC.

Procedure

Step 1   Dial a conference on the Cisco IPVC 35xx MCU from a SIP endpoint by dialing the conference ID and default domain.

For example, dial:

601234@default.domain

Whereas:

- 602134—Cisco IPVC 35xx MCU conference ID (service prefix + unique conference identifier)
- default.domain—Default domain of the Cisco IPVC 35xx MCU on which the conference is hosted.

Dialing into the Cisco IPVC 35xx MCU Configured as a Separate SIP Domain from a UAC

Administrators can configure a Cisco IPVC 35xx MCU as a separate SIP domain. Users can start or join an ad hoc conference by dialing into this Cisco IPVC 35xx MCU from a SIP-complaint endpoint called a User Agent Client (UAC).

Procedure

Step 1   Dial the conference ID and the unique Cisco IPVC 35xx MCU domain as defined in the proxy or Domain Name Server (DNS) server.

For example, dial:

conference.id@mcu.domain.com

Using Dialing Conventions with IP Endpoints

You can start or join an ad hoc conference from any IP-based endpoint. When dialing from an IP endpoint, configure the dialing software, IP phone, or other device with the appropriate network configuration details (H.323 gatekeeper IP address or SIP proxy IP).

Procedure

Step 1   To start or join a conference with IP endpoint, choose one of the following steps:

   a. To start or join a conference, dial the conference ID number.

      For example, dial 601234.

      As soon as the Cisco IPVC 35xx MCU accepts the call, you connect to the existing conference or the Cisco IPVC 35xx MCU creates a new conference with this conference identifier.

   b. To start or join a conference and invite a participant, dial the conference ID number followed by the invite sign (**) and the number of the participant you want to invite.

      For example, dial 601234**5678

      As soon as the Cisco IPVC 35xx MCU accepts the call, you connect to the existing conference or the Cisco IPVC 35xx MCU creates a new conference with this conference identifier.

   c. To start or join a conference and invite a participant on the Integrated Services Digital Network (ISDN), Public Switched Telephone Network (PSTN) or cell phone network, dial the conference ID number followed by the invite sign (**), the appropriate gateway service prefix, ISDN line.

      For example, dial 601234**867655001 (<Conference ID number> + <**> + <Gateway service prefix + line number>).

      As soon as the Cisco IPVC 35xx MCU accepts the call, you are connected to the existing conference or a new conference is created with this conference identifier.

About Controlling Conferences with DTMF

Note   Note: This section applies to Release 4.1 only

You can control a Cisco IPVC 35xx MCU conference using Dual Tone Multi-Frequency (DTMF) signals from an endpoint during that conference. You can use this functionality to join an audio bridge to your video and voice conference by cascading.

The Cisco IPVC 35xx MCU passes out-of-band DTMF signals transparently to gateways. The gateway inserts in-band signals on receiving the DTMF from the Cisco IPVC 35xx MCU. The audio bridge receives these in-band signals and responds accordingly.

Table 4-1 shows available DTMF control signals

Table 4-1   DTMF Controls

During a conference press * followed by:	
*	Listen to available options
1	Take/release Chair Control.
2	Mute/unmute your line.
3	Control your volume.
7	Block/unblock admission to conference (for Chair Control-level users only).

Table 4-1   DTMF Controls

During a conference press * followed by:	
8	Invite a new participant (for Chair Control-level users only).
#	Exit this menu.

About Two-Stage Dialing

> **Note**   This section applies to Release 4.1 only.

To control conferences using DTMF, callers use a two-stage dialing process to invite an audio bridge to a conference:

- Dialing stage 1—The Cisco IPVC 35xx MCU prompts a conference participant to take Chair Control. The participant then dials the audio bridge telephone E.164 number using DTMF control signals from the remote control of the video endpoint. The Cisco IPVC 35xx MCU recognizes the DTMF-based request and connects to the audio bridge.

- Dialing stage 2—The calling participant is prompted by a remote IVR to dial the ID of the required conference.

> **Note**   Endpoints must support out-of-band DTMF signaling for two-stage dialing to succeed.

Once the Cisco IPVC 35xx MCU connects with the audio bridge, the Interactive Voice Response (IVR) mechanism in the audio bridge plays a message prompting the caller to input additional digits. For example:

- "Press 1 to join a meeting."

- "Enter the meeting ID now then press #."

- "At the tone, please state your name then press #."

- "to join your meeting, please press 1 now."

About DTMF Forwarding

> **Note**   This section applies only to Release 4.1.

DTMF forwarding can forward DTMF signals to:

- Connected gateways only

- All endpoints connected to the conference

You can also choose to disable DTMF signals. DTMF forwarding is disabled by default.

You configure DTMF forwarding settings using the DTMF forwarding advanced command. See the"Sending Advanced Commands" section on page 3-20 for more information.

The DTMF forwarding algorithm responds to the values configured in the DTMF forwarding advanced command and for the Enable DTMF Conference control setting in the DTMF Control section of the Settings tab (See the "Configuring DTMF Control" section on page 3-8). Table 4-3 explains the DTMF forwarding algorithm.

Table 4-2   DTMF Forwarding Algorithm

DTMF forwarding Advanced Command	Enable DTMF Conference control Setting	Result
to all	unselected	All DTMF tones are sent.
to all, to gateways	selected	Only DTMF tones entered after dialing *8 and the destination e.164 number (i.e. instructions which are sent after the call has left the Cisco IPVC 35xx MCU).

About DTMF XML Notification

Note   This section applies to Release 4.1.

You configure the behavior the Cisco IPVC 35xx MCU when using DTMF XML notifications through the Handle DTMF after XML notification advanced command. See the "Sending Advanced Commands" section on page 3-20 for more information.

About Cisco IPVC 35xx MCU Access Levels

There are four ways to interact with the Cisco IPVC 35xx MCU user interfaces according to the following access levels:

- Administrator
- Operator
- Chair Control
- User

Administrator- and Chair Control-configured password settings as well as conference password settings. determine access levels.

Table 4-3 describes each access level.

Table 4-3   Cisco IPVC 35xx MCU Access Levels

Access Level	Privileges
Administrator	- Full access to the Cisco IPVC 35xx MCU Administrator interface. - Full Operator-level access to the Conference Control interface.

Table 4-3   *Cisco IPVC 35xx MCU Access Levels*

Operator	• Access to the Conference Control interface using the Create Conference window. • Access to view details of all conferences hosted on the Cisco IPVC 35xx MCU and to cascaded conferences hosted on participating Cisco IPVC 35xx MCUs. • Ability to create a new conference from the Conference Control access window, the Create Conference window, or the Conference Control interface. • Chair Control-level access to all conferences while chair control is simultaneously held by other users. • Ability to invite other participants to a conference.
Chair Control	• Access to view conference details of conferences hosted on the Cisco IPVC 35xx MCU and to cascaded conferences hosted on participating Cisco IPVC 35xx MCUs for which access authorization is granted. • Chair Control level-access to conferences when the user has a valid Chair Control password or the conference chair is not held by another user. • Ability to invite other participants to a conference.
User	• View-only access to conferences hosted on the Cisco IPVC 35xx MCU for which authorization is granted. • Ability to invite other participants to a conference.

About the Create Conference Window

The Create Conference window is accessible for users with Operator-level access. Operators can use the Create Conference window to select conferences to monitor and control from the list of conferences currently running, or create a new conference.

The number of currently-running conferences appears in the Number of Conferences field. The Create Conference window displays information about each conference in a table format with the following columns:

• Conference ID—Conference ID number. Each ID number is a hyperlink that you can select to display the Conference Control interface for that conference.

- Description—Description of the conference entered by the user who created it. For Release 4.1 only, an error symbol appears if an MP failure occurs.

- Number of participants—The number of participants currently attending the conference.

- Media Types—Icons indicate the type of media supported by the conference: voice, video, and data.

- Encryption Mode—Indicates the level of encryption currently in use for the conference: best effort, encryption required, or strong encryption required.

Figure 4-1 and Table 4-4 show and lists the elements in the Create Conference window.

Figure 4-1   Create Conference Window Elements

Table 4-4   Create Conference Window Elements

Number	Description
1	Sign out button
2	Help button
3	Cancel button
4	Advanced button
5	Create button

Accessing the Create Conference Window

All users can access the Cisco IPVC 35xx MCU Create Conference window using the
Cisco IPVC 35xx MCU Conference Control access window where they can join an existing conference
or create a new conference. With an appropriate access level, they can also use this window to sign in as
an Administrator or Operator to configure the Cisco IPVC 35xx MCU or manage multiple conferences.

Procedure

Step 1   Access the Cisco IPVC 35xx MCU access window.

Step 2   Click **Enter a conference**.

The Cisco IPVC 35xx MCU Conference Control access window appears.

Step 3   To monitor a conference, follow these steps:

a.   In the **Conference ID** field, enter the number of the conference you want to monitor.

b.   In the **Password** field, enter the password for the conference you want to monitor.

To create a new conference, follow these steps:

a.   Click the **Create conference** button.

To sign in with Operator or Administrator authorization:

a.   Click **Sign in**.

Viewing Online Help from the Conference Control Window

You can view online help about the Create Conference window.

Procedure

Step 1   In the Create Conference window, on the control bar, click **Help**.

Creating Conferences from the Create Conference Window

Users with Chair Control-level access or Administrators can create a conference using available
predefined services in the Create Conference window. Such users can also optionally set a password for
accessing the new conference and a password for obtaining Chair Control of the new conference.

Before You Begin

Have an Administrator configure Cisco IPVC 35xx MCU services if there are not already existing ones.

Procedure

Step 1   Launch your browser and enter the IP address of the Cisco IPVC 35xx MCU.

The Cisco IPVC 35xx MCU access window appears.

Step 2   Click **Enter a Conference**.

The Cisco IPVC 35xx MCU Conference Control access window appears.

Step 3   Click **Create conference**.

The Create Conference window appears, displaying available pre-configured service prefixes and their descriptions.

Step 4   Choose a service prefix from the list of pre-configured ones.

The prefix appears in the Prefix field.

Step 5   In the **Unique Number** field, enter a number for this conference.

> **Note**   You cannot use an existing conference number.

Step 6   (Optional) In the **Conference Password** field, enter a password used for accessing the conference.

Step 7   (Optional) In the **Chair Password** field, enter a password used for obtaining Chair Control in the new conference.

> **Note**   You can also configure a default Chair Control password for a service profile in the Administrator interface.

Step 8   (Optional) In the **Conference Description** field, you can enter text describing the conference that appears in the Create Conference window.

Step 9   (Optional) You can configure additional settings for a new conference such as conference duration, time-out, and dialing policy settings:

   a.   Click the **Advanced** button.

   The Advanced Features dialog box appears.

   b.   (Optional) In the Conference Duration section, click the **Unlimited** radio button or click the **Min** radio button and set time limitation (in minutes) for the conference.

   c.   (Optional) Select the **Terminate Conference when empty** check box to end a conference it is vacant for the number of minutes you enter in the field in this setting.

   d.   (Optional) Select the **Disallow dial-in to the conference** check box to prevent participants dialing in to the conference. Attendance is thus by invitation only. This ensures that users dialing the wrong number do not join this conference by mistake.

   e.   Click **OK**.

Step 10   Click **Create**.

> **Note**   If an error message appears, stating that no resources are available, check whether the appropriate MP (including the
> Cisco IPVC 3540 Application Server (AS) Module for Data Collaboration Server (DCS),
> Enhanced Media Processor (EMP), Rate Matching Module, and local Cisco IPVC 35xx MCU
> MP unit) is registered or online in the Registered MPs tab in the Administrator interface.

Terminating Conferences

You can disconnect an inactive or unused conference in the Create Conference window.

Procedure

Step 1   In the Create Conference window, click the Terminate Conference icon next to the conference name to end the conference.

Signing Out of the Create Conference Window

You can exit the Create Conference window.

Procedure

Step 1   In the Create Conference window, on the control bar, click **Sign out**.

About the Conference Control Interface

From the Cisco IPVC 35xx MCU Conference Control interface, you can:

- View active conferences hosted on the Cisco IPVC 35xx MCU or on cascaded Cisco IPVC 35xx MCUs.
- View conference participant details
- Create conferences
- Control conference connections
- Monitor and manage conference behavior

While all users can view the Conference Control interface, access to conference management features is controlled by authorization access levels: Administrator, Operator, Chair Control, and User.

Note   For Release 4.1, the Conference Control interface is best viewed in full screen mode (1024 x 768 fps).

Note   For Release 4.1, you can view multiple Conference Control interface browser windows at the same time to monitor different conferences. We recommend, however, that you close windows you are not currently viewing to avoid confusion and perform operations in the wrong conference.

Figure 4-2 and Table 4-5 show and list the elements of the Conference Control interface.

Figure 4-2   Conference Control Interface Elements
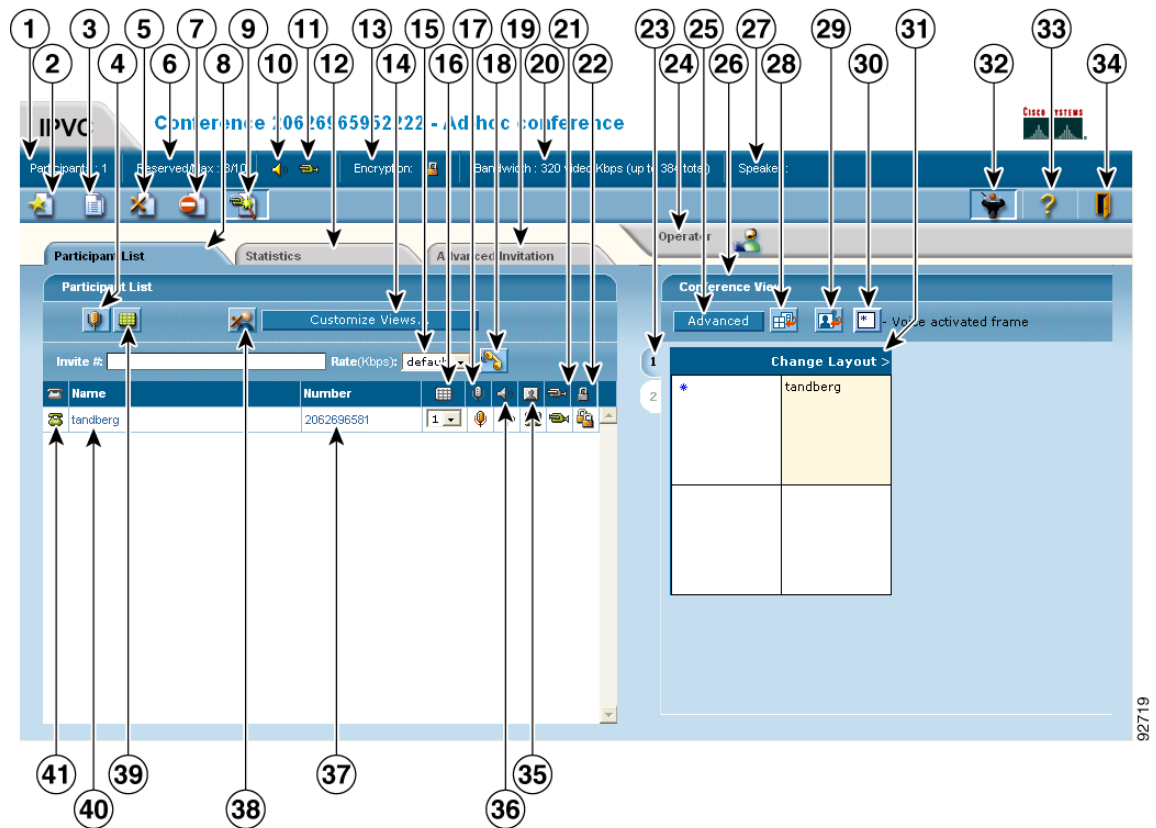
Table 4-5   Conference Control Interface Elements

Number	Description
1	Participants field. Displays number of participants in the current conference.
2	Create Conference button.
3	View Conference List button. Click to view the Create Conference window. See the "About the Create Conference Window" section on page 4-8 for more information.
4	Mute/Unmute button.
5	Terminate Conference button.
6	Reserved/Max field. Displays the reserved number of participants and maximum number of participants for this conference.
7	Conference Admission button.
8	Participant List tab.
9	Enable/Disable QualiVision button.
10	Media type icon indicating that this conference supports voice. For Release 4.1 only, an error symbol appears if an MP failure occurs.
11	Media type icon indicating that this conference supports video. For Release 4.1, an error symbol appears if an MP failure occurs.
12	Statistics tab.

Table 4-5   *Conference Control Interface Elements*

Number	Description
13	Encryption field. Displays the level of encryption for this conference: best effort, encryption required, or strong encryption required.
14	Customize Views button.
15	Rate(Kbps) field.
16	Location in View column. Indicates the conference view displayed to the participants.
17	Audio In column. Displays Mute icons for participants whose audio is not muted and Unmute icons for participants whose audio is muted.
18	Invite button.
19	Advanced Invitation tab.
20	Bandwidth field. Displays the bandwidth the current conference is using.
21	Video Image column. Displays Video Image icons that indicate whether the video stream from the participant to the Cisco IPVC 35xx MCU is enabled or blocked. If the Video Image icon has a star, then QualiVision is enabled for the video stream from the participant to the Cisco IPVC 35xx MCU.
22	Encryption column. Displays the level of encryption that the endpoints require: best effort, encryption required, or strong encryption required.
23	Layout display frame.
24	Operator button.
25	Advanced button.
26	Conference View section.
27	Speaker field. Displays the participant currently speaking in the conference.
28	Dynamic Layout button.
29	Auto-switch button.
30	Voice activated frame button.
31	Change Layout button.
32	Take Control/Release Control button.
33	Help button.
34	Sign out button.
35	Video Display column. Displays Video Display icons that indicate whether the conference video display sent to the participants is enabled or blocked. If the Video Display icon has a star, then QualiVision is enabled for the video stream from the Cisco IPVC 35xx MCU to the participant.

Table 4-5   Conference Control Interface Elements

Number	Description
36	Audio Out column. Displays Audio Out icons that indicate whether the conference audio connection to the participants are enabled or muted.
37	Number column. Displays the endpoint numbers of the conference participants.
38	Delete Participant button.
39	Change Participant View button.
40	Name column. Displays the names of the endpoint.
41	Participant connection status icons: Connected, Disconnecting, or Disconnected.

The following sections describe the tasks that users with appropriate access levels can perform in the Conference Control Interface:

- Accessing the Conference Control Interface, page 4-15
- Refreshing the Conference Control Interface, page 4-16 (Release 4.1 only)
- Viewing Online Help from the Conference Control Interface, page 4-16
- Taking and Releasing Chair Control, page 4-17
- Creating Conferences from the Conference Control Interface, page 4-17
- Inviting an Operator to a Conference, page 4-17
- Enabling and Disabling QualiVision, page 4-18
- Configuring T.120 Data Collaboration, page 4-18
- Configuring Participant Settings, page 4-19

Accessing the Conference Control Interface

You can access the Conference Control interface from any Java-enabled web browser.

Procedure

Step 1   Access the Cisco IPVC 35xx MCU interface.

✎

Note   For Release 4.1, the Conference Control interface is best viewed in full screen mode (1024 x 768 fps).

Step 2   Click **Enter a conference**.

The Cisco IPVC 35xx MCU Conference Control access window appears.

Step 3   Choose one of the following two methods.

To access an existing conference:

a. In the **Conference ID** field, enter the conference ID.

b. In the **Password** field, enter the password, if applicable.

c. Click **Go**.

–or–

To create a new conference:

a. Click the **Create conference** button.

The Create Conference window appears.

b. Choose a service prefix from the list of pre-configured ones

c. In the **Unique Number** field, enter a unique number for the conference.

> ✎
> **Note** You cannot use a number already in use by another conference.

d. Click **Create**.

Refreshing the Conference Control Interface

> ✎
> **Note** This section applies only to Release 4.1.

The Conference Control interface refreshes itself every 10 seconds to provide updated information. To refresh information instantly, click the tab in the interface that you are viewing.

> ✎
> **Note** Do not click the Refresh button in your web browser: this exits the Conference Control interface and returns you to the access window.

For Microsoft Windows systems, if you have enabled the Start Navigation sound, and a continuous clicking sound is heard when the Conference Control interface automatically refreshes, disable this setting in the Sounds and Multimedia section of the Control Panel.

Viewing Online Help from the Conference Control Interface

You can view help information for a selected tab in the Conference Control interface.

Procedure

Step 1 In the Conference Control interface, click the tab you want tho view help information for: **Participant List**, **Statistics**, or **Advanced Invitation**.

Step 2 Click **Help**.

Taking and Releasing Chair Control

With Chair Control-level access, for conferences already in progress, you can control conference activity and initiate events such as inviting participants. When you obtain Chair Control, you can edit participant connections, create new conferences, and audio sub-conferences, and change video layout and the position of participant images. You can block conference admission, block audio and video streams, and terminate the conference. You can split the existing conference and transfer some participants to the new conference. Chair control access also provides additional viewing and configuration options in the Conference Control interface.

Chair Control access can be password protected. Administrators and Operators can jointly hold Chair Control simultaneously.

Procedure

Step 1   In the Conference Control interface, click **Take Control** to take control of that conference.

Step 2   A dialog box requesting a password might appear if chair control access is password-protected. Enter the password.

Step 3   To release control of the conference, click the **Release Control** button.

Creating Conferences from the Conference Control Interface

Chair Controls, Operators, and Administrators can create a new conference from the Conference Control interface.

Procedure

Step 1   In the Conference Control interface, click **Create Conference**.

Step 2   The Create Conference window appears.

Step 3   Follow the steps in the "Creating Conferences from the Create Conference Window" section on page 4-10.

Inviting an Operator to a Conference

Users with Chair Control-level access can invite an Operator to join a conference to answer questions and provide support. An Administrator pre-configures the Operator number.

Note   If an Operator is not pre-configured by an Administrator, the call to the Operator does not connect.

Procedure

Step 1   In the Conference Control interface, click **Operator**.

The Operator appears in the Participant List.

Enabling and Disabling QualiVision

In the Conference Control interface, users with Chair Control-level access can enable or disable the QualiVision feature for a current conference. The QualiVision feature provides improved video quality in networks with up to 7% packet loss.

Before You Begin

Configure QualiVision settings in the Administrator interface.

Procedure

Step 1   On the control bar, click **QualiVision** to enable (if not already selected) or disable (if already selected) QualiVision.

Configuring T.120 Data Collaboration

From the Conference Control interface, users with Chair Control-level access can open a T.120 data sharing session in Microsoft NetMeeting or join a session if one already exists for the conference. T.120 data collaboration over the video conference connection enhances the conference by providing data-sharing tools. Participants in a T.120 data collaboration video conference can simultaneously view diagrams, graphic presentations, and slide lectures. In addition, private text chats, white board exchanges, or rapid file transfers can occur while the video conference proceeds.

The Cisco IPVC 3540 Application Server (AS) Module for Data Collaboration Server (DCS) provides support for T.120 data collaboration. This module can support many conferences and Cisco IPVC 35xx MCUs at the same time while remaining transparent to the participants of individual conferences.

The sequence of events, shown in Figure 4-3, describes how a T.120-enabled H.323 endpoint creates a T.120 data collaboration session during a video conference:

Figure 4-3   Connection Process for Data Collaboration Server (DCS)
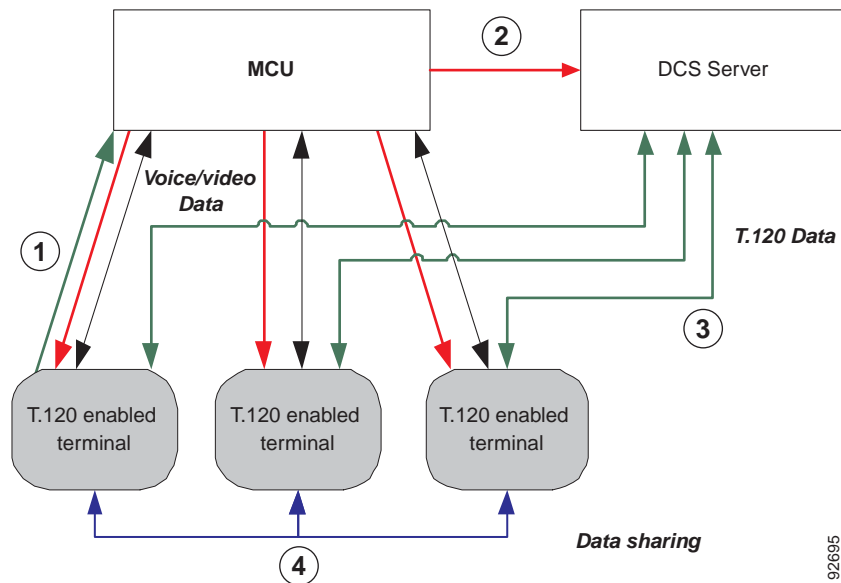
Note T.120 must be enabled in the Cisco IPVC 35xx MCU service.

1. The endpoint requests data collaboration services.

2. The Cisco IPVC 35xx MCU simultaneously relays a T.120 connection request to the DCS and sends connection information to the endpoint.

3. The DCS opens data sharing channels between the endpoints.

4. All T.120 enabled endpoints in the conference connect in a data sharing session.

The Cisco IPVC 3540 Application Server (AS) Module for Data Collaboration Server (DCS) supports T.120 data collaboration across a cascaded video conference.

Users with Chair Control-level access can set up a T.120 data conference in the Conference Control interface.

Procedure

Step 1   Click the **Join Data Conference** button.

Configuring Participant Settings

The Participant List tab in the Conference Control interface contains the following sections:

- Participant List section, which displays information about conference participants. Users with Chair Control-level access can view and edit media connections for each participant. Table 4-6 describes the information that appears in the Participants List section.

- Conference Views section, which displays information about the conference layout and view.

Table 4-6   Participants List Section Columns

Column	Description
Status	Displays status icons for the connection status of each conference participant. The following image shows the icons for connected, connecting, and disconnected. Disconnected participants remain in the Participant List for the duration of the conference, enabling you to reconnect participants without sending repeat invitations. You can rearrange the list of participants in the Participant List by clicking the icon in the title of this column.
Name	The name of the conference participant. This column can include: • The dial out icon to indicate that the Cisco IPVC 35xx MCU invited the specified participant. • The current speaker indication icon that indicates that the specified participant is currently the active speaker. • Video quality warning icons—medium or poor video quality—that indicate the current quality of the IP network video connection for the participant.
Number	The participant's endpoint number.
Change Participant View	Button that appears when the conference supports multiple views. You can click this button to change the conference view layout for the participant.
Location in View	Indicates the conference view that appears to the participant. When the conference is configured with more than one view, you can choose available views from a list.
Select Layout	Indicates the number of the video layout displayed to the participant upon entry to the conference. This column appears only when viewing sub-conference details.
Audio In	Indicates whether the voice of the selected participant is muted or enabled.

Table 4-6   Participants List Section Columns

Column	Description
Audio Out	Indicates whether the conference audio connection is muted or enabled.
Video Image	Indicates whether the video stream that the participant is sending is blocked or unblocked.
Video Display	Indicates whether the conference video display sent to the participant is blocked or unblocked. If the icon contains a star, then QualiVision is enabled for the video stream from the Cisco IPVC 35xx MCU to the participant.
Data Sharing	Indicates that the participant supports T.120 data sharing.

The following sections describe the task that users with appropriate access level can perform in the Participant List tab:

- Muting and Unmuting Participant Audio Connections, page 4-21
- Configuring Manual Gain Control Using the Web, page 4-22 (Release 4.1 only)
- Changing Participant Views, page 4-22
- Blocking the Video Stream, page 4-23
- Enabling or Disabling Dynamic Layouts, page 4-24
- Displaying Participant Names in Frames, page 4-24
- Enabling or Disabling Auto-Switch Mode, page 4-24
- Changing Conference Layouts, page 4-25
- Configuring Conference Advanced View Settings, page 4-25
- Viewing Conference Statistics, page 4-25
- Customizing Views, page 4-26
- Using Quick Invites to Invite Conference Participants, page 4-29
- Reconnecting Participants, page 4-30
- Blocking Conference Admission, page 4-31
- Deleting Conference Participants, page 4-31

Muting and Unmuting Participant Audio Connections

In the Participant List tab, users with Chair Control-level access can mute or enable the audio connection to the conference of all participants in the conference.

Procedure

Step 1   On the control bar, click **Mute** to mute all participants or **Unmute** to enable the audio connection for all participants.

Users with Chair Control-level access can also mute or enable the audio connection of an individual participant in a conference.

Procedure

Step 1   In the Participants List section, select a participant.

Step 2   In the Audio In column, click the **Mute** or **Unmute** icon.

Configuring Manual Gain Control Using the Web

Note   This section applies only to Release 4.1.

In the Conference Control interface, you can control the volume of participating endpoints (manual gain control) in a conference. For a regular conference, your setting only affects the location that is connected to a specific Cisco IPVC 35xx MCU port. In a cascaded conference, changing this setting affects all remote participants on other Cisco IPVC 35xx MCUs. Once you change this setting, the new setting remains in effect until that endpoint leaves the CCisco IPVC 35xx MCU.

Before You Begin

You must have Chair Control-level access to configure manual gain control.

Procedure

Step 1   In the **Participant List** tab, right-click the participant you want to change the volume for and choose **Change volume**.

Step 2   The gain control scroll bar dialog box appears, with a gain span of -5 to 5.

Step 3   Drag the scroll bar to the right to increase the gain; drag the slide bar to the left to decrease the gain.

Step 4   Close the gain control slide bar dialog box.

.

Changing Participant Views

In the Participant List tab, if a conference supports multiple views, users with Chair Control-level access can change the conference view layout for an individual conference participant or all conference participants while the conference is in progress.

Procedure

Step 1   (Optional) If you want to change the conference view layout for an individual conference participant, click that participant in the Participant List section.

Step 2   In the Participant List section, select a participant.

Step 3   Click **Change Participant View**.

The Change Participants View dialog box appears.

Step 4   Choose the **All** radio button.

Step 5   Click **OK**.

Configuring Sub-Conferences

In the Participant List tab, users with Chair Control-level access can create a sub-conference within a conference. The Cisco IPVC 35xx MCU supports audio sub-conferences to which the Chair Control can divert selected participants in the existing conference to a private audio sub-conference session. The connection to the main conference remains active. The Cisco IPVC 35xx MCU hides sub-conference session participants from the other participants in the video layout. They can return to the conference at any time and reoccupy any previously held positions in the main conference video display. While in a sub-conference, participants can continue viewing and hearing the main conference.

Note   This option is available only when a conference is configured to support sub-conferences

Procedure.

Step 1   In the Participant List section, click a participant.

The Select sub-conference dialog box appears.

Step 2   From the list, select the required sub-conference.

Step 3   Click **Ok**.

A new Sub-conf column appears in the Participant List with a list of all available sub-conferences for that participant.

Step 4   In the Sub-conf column, select a sub-conference for that participant.

Step 5   To return the participant to the main conference, in the Sub-conf list, select **Main**.

When all participants return to the main conference and none remain in the sub-conference, the Sub-conf column disappears from the Participant List.

Blocking the Video Stream

In the Participant List tab, users with Chair Control-level access can block the video stream sent by a participant to a conference. For example, a participant video connection might affect conference processing and degrade performance. You can block the participant's video until problems at the participant's endpoint are resolved.

Procedure

Step 1   In the Participant List section, click the Video Image icon.

Enabling or Disabling Dynamic Layouts

In the Participant List tab, users with Chair Control-level access can enable or disable dynamic layouts for a conference. A dynamic layout seamlessly switches the conference video image between a wide range of layouts to correspond with the number of participants in attendance at any given time during the conference. The video image switches to a layout with frames equal to the number of participant images, to a maximum of 16. The layout changes accordingly as participants join or leave a conference.

A dynamic layout conserves bandwidth, eliminates the display of empty frames in the video image, and makes optimum use of the video image for displaying participant images. This type of layout switching is suitable for a conference with a high rate of participant traffic joining and leaving the conference or an adaptive service used for a variety of conference sizes.

Note This feature is available with Enhanced Media Processor (EMP) support.

Procedure

Step 1 In the Conference View section of the Participant List tab, click **Dynamic Layout** to enable (if not selected) or disable (if already selected) dynamic layout for this conference.

Displaying Participant Names in Frames

In the Participant List tab, users with Chair Control-level access can choose to display the name of endpoints or participants in specific positions of the video layout frame.

Before You Begin

This feature is visible only with EMP support and when you configure text overlay in the service.

Procedure

Step 1 In the Conference View section of the Participant List tab, click **Display participant names in frame**.

Enabling or Disabling Auto-Switch Mode

In the Participant List tab, users with Chair Control-level access can enable the auto-switch mode for a conference. The auto-switch mode displays all the participants of a large conference in Continuous Presence (CP) mode display in the video layout on a rotating basis. Participant images can be replaced at preset intervals.

Procedure

Step 1 In the Conference View section of the Participant List tab, click **Auto-switch** (if not already selected) to enable or disable (if already selected) auto-switch mode.

Changing Conference Layouts

In the Participant List tab, users with Chair Control-level access can change the layout for the current conference.

Procedure

Step 1   In the Conference View section of the Participant List tab, click **Change Layout**.

A dialog box appears, displaying a list of currently available layouts for the current conference.

Step 2   Choose a layout.

The conference adjusts to the new selection.

Configuring Conference Advanced View Settings

In the Participant List tab, users with Chair Control-level access can view advanced view settings for a conference. Users with Chair Control-level access can also configure outgoing bandwidth settings.

Procedure

Step 1   In the Conference View section of the Participant List tab, click the **Advanced** button.

The Advanced Setting dialog box appears, displaying the following columns:

- Video Scheme—Displays the number of the conference view. A conference view can support up to four video layouts or video schemes.
- Bandwidth—Displays the maximum outgoing bandwidth of the conference view. You can edit this setting.
- Frame Rate—Displays the number of frames per second that the conference view supports.
- Video Codec—Displays the video codec that the conference view supports.
- Picture Size—Displays the image resolution that the conference view supports.

Step 2   In the **Bandwidth** column, click in the text field and enter a bandwidth in Kbps.

Step 3   Click the **ok** button in this row to apply your setting.

Step 4   Click **OK** to close the Advanced Setting dialog box.

Viewing Conference Statistics

For users with Chair Control-level access, the Statistics tab of the Conference Control interface displays a comprehensive set of statistical information about bandwidth usage and audio/video packet behavior. Statistics frequently update automatically and enable you to monitor conference performance.

Table 4-7 lists the fields that appear in the Statistics tab.

Table 4-7   Statistics Tab Fields

Field	Description
Video byes in/out	The total value of incoming video bytes from all participants in the conference.
Audio bytes in/out	Total value of incoming audio bytes from all participants in the conference.
Lost packets Video/Audio	Total number of lost audio and video packets from all participants in the conference.
Abnormal disconnections	The number of abnormal participant disconnections during the current conference.
Conference duration	The length of time the conference has been active.
Packets reordered	The number of packets that the Cisco IPVC 35xx MCU has reordered during the current conference.
Intra request counter	The number of Fast Update requests that the Cisco IPVC 35xx MCU sent.
Jitter buffer maximum size (Video/Audio)	The maximum size of the Jitter buffer for accumulating IP packets.
Jitter buffer current size (Video/Audio)	The current size of the Jitter buffer for accumulating IP packets.
Jitter buffer minimum size (Video/Audio)	The minimum size of the Jitter buffer for accumulating IP packets.

Related Topics

Updating Conference Statistics

In the Participant List tab, users with Chair Control-level access can manually update statistics appearing in the Statistics tab.

Procedure

Step 1   In the Statistics tab, click **Update**.

Related Topics

Customizing Views

Users with Chair Control-level access can view extended statistical information about participant connections, bandwidth usage, and audio and video problems in the Participant List tab. Table 4-8 explains the additional categories of information you can display.

Table 4-8   *Customized Participant List Categories*

Category	Additional Information Displayed in Participant List
Participant Extended Info	Includes the following columns: • IP Address—Participant endpoint IP address. • Type—Participant endpoint type. • Description—Participant description (displays the endpoint vendor identifier, if available). • Connect Time—Time at which the participant connected to the conference. • Video In/Out—Video formats the participant is sending and receiving. • Audio In/Out—Audio codecs the participant is sending and receiving. • Data—Indicates whether the participant is participating in data sharing.
Video Statistics	Includes the following columns: • Total BW In/Out—Total bandwidth sent and received by the participant. • Data IP—IP address of the participant data sharing terminal. • VFU Req. In/Out—Total Video Fast Update (VFU) requests sent and received by the participant. • Video BW In/Out—Total video bandwidth sent and received by the participant. • Video Packets In/Out—Total video packets sent and received by the participant. • Video Bytes In/Out—Total bytes of video sent and received by the participant. • Video Out Addr.—IP address and port to which video is sent to the participant. • Fps In/Out—Frame rate of video sent and received by the participant. • Pic. size In/Out—Picture size of video sent and received by the participant. • Video Jitter In: current/min/max—Accumulated video packets received from the participant. Includes the current value and average values for the minimum and maximum number of packets received from the participant.

Table 4-8   *Customized Participant List Categories*

Category	Additional Information Displayed in Participant List
Audio Statistics	Includes the following columns: • Audio BW In/Out—Total audio bandwidth sent and received by the participant. • Audio Intra Request Counter In/Out—Total audio fast update requests sent and received by the participant. • Audio Packets In/Out—Total audio packets sent and received by the participant. • Audio Bytes In/Out—Total audio bytes sent and received by the participant. • Audio Out addr.—IP address and port to which audio is sent to the participant. • Audio Jitter Buffer In: current/min/max—Accumulated audio packets received from the participant. Includes the current value and average values for the minimum and maximum number of packets received from the participant.
Video Problems	Includes the following columns: • Video Out of Order Packets—Total video packets sent to and received from the participant out of sequence. • Video Lost Packet In/Out—Total lost video packets sent to and received from the participant.
Audio Problems	Includes the following columns: • Audio Out of Order Packets—Total audio packets sent to and received from the participant out of sequence. • Audio Lost Packet In/Out—Total lost audio packets sent to and received from the participant.

Procedure

Step 1   In the Participants List tab, click **Customize Views**.

The Customize Views dialog box appears.

Step 2   Select or unselect the check boxes for the categories of additional information that you want to appear or remove in the Participant List:

- Participant Extended Info
- Video Statistics
- Audio Statistics
- Video Problems
- Audio Problems

You can click **Select all** to select all categories; likewise, you can click **Clear all** to remove all categories from the Participant List.

Step 3   Click **OK**.

Using Quick Invites to Invite Conference Participants

In the Participant List tab of the Conference Control interface, all users can use the quick invite feature to send an invitation to participate in a conference.

Procedure

Step 1   In the **Invite #** field, enter the participant number you want to invite. You can invite multiple participants by separating them with the invite sign (**).

Step 2   (Optional) You can select a bandwidth rate lower than the current conference rate at which the invited participant joins the conference. You can thus invite individual participants with lower connection capabilities. In the **Rate(kbps)** field, choose a new bandwidth rate.

Step 3   Click **Invite**.

Related Topics

- Inviting Participants with Advanced Settings, page 4-29

Inviting Participants with Advanced Settings

All users can invite multiple participants into a conference at the same time in the Advanced Invitation tab of the Conference Control interface. As each invite field can accommodate multiple participant numbers with separators, you can use this tab to invite a large number of participants at the same time. All users can also select a lower bandwidth rate with which to connect individual participants.

In the Advanced Invitation tab, all users can also drag and drop participant images into preferred positions in the layout of each conference view that the conference supports. All users can also set the layout which invited participants see when joining a conference.

In a cascaded conference, all users can choose which Cisco IPVC 35xx MCU actually invites the participant.

Procedure

Step 1   In the Conference Control interface, click the **Advanced Invitation** tab.

Step 2   In the first **Invite #** field, enter the participant contact numbers. You can enter multiple numbers separated by the invite sign (**).

Step 3   In the **Display Name** field, enter the name you want to appear when the participant enters the conference.

Step 4   In the **Kbps** field, choose the bit rate that the Cisco IPVC 35xx MCU uses when inviting a participant to a conference. Choose **default** for optimal bit rate performance.

Step 5   In the **MCU** field, choose a cascaded Cisco IPVC 35xx MCU conference to which invited participants connect.

Note   This step is only for cascaded conferences.

Step 6   (Optional) To configure advanced features, follow these additional steps;

    a. Click **Advanced**.

       Additional control features appear in the Advanced Invitation tab.

    b. Click **Change Layout**.

       A dialog box appears displaying a list of the current layouts available in the current conference.

    c. Drag and drop the **Voice activated frame** button into the preferred position in the **Layout display frame** that appears in the Conference View section.

> **Note**   You can set a position for the participant image in all layouts that the conference currently supports.

    d. At the end of each participant row, choose from the list the number of the conference video layout you want to display to the participant upon entry into the conference. Choose **L** to display the local view of a slave conference.

       A slave conference on an EMP-enabled Cisco IPVC 35xx MCU has two views:

        – The local (slave Cisco IPVC 35xx MCU conference) CP view

        – The view that the master Cisco IPVC 35xx MCU broadcasts.

       An Operator of the slave conference should be able to switch the view for each participant in the slave conference so that the participant can see the view broadcasted by the master or the local view. This feature is useful in large cascaded conferences where each site has a local operator. Most participants at the local site see the view broadcasted by the master Cisco IPVC 35xx MCU, but the local operator can see the local view of local participants.

       You can enable a local view of a slave conference in the Edit View dialog box.

Step 7   Repeat steps 1-6 for each **Invite #** field until you configure all required the participant invites.

Step 8   Click **Invite** to send the invitations.

Related Topics

- Using Quick Invites to Invite Conference Participants, page 4-29

Reconnecting Participants

If participants are disconnected from a conference, users with Chair Control-level access can reconnect them in the Participant List tab.

> **Note**   When the Enable auto-reconnect option is configured in the conference service, then the Cisco IPVC 35xx MCU automatically calls disconnected terminals to attempt a reconnection.

Procedure

Step 1   In the Participant List tab, click the **Disconnect** icon to attempt a reconnection.

Blocking Conference Admission

Users with Chair Control-level access can block the admission of additional participants in a conference in the Conference Control interface.

Procedure

Step 1   On the Control Bar, click **Conference Admission**.

No further participants can join the conference. To readmit participants, click **Conference Admission** again.

Deleting Conference Participants

In the Participant List tab, users with Chair Control-level access can remove participants from conferences.

Procedure

Step 1   In the Participants List section, click the participant you want to remove.

Step 2   On the control bar, click **Delete Participant**.

Cascading Conferences

Users with Chair Control-level access can increase Cisco IPVC 35xx MCU call capacity by cascading Cisco IPVC 35xx MCUs. This option supports the bridging of several separate conferences to create very large conferences through IP connections (H.323 and SIP) and also through ISDN/PSTN connections (H.320) when operating in conjunction with a gateway.

In the Conference Control interface, cascading a conference works the same way as inviting a single participant into an existing conference. Once you create a cascaded conference, you can use the Cisco IPVC 35xx MCU to set the conference to which invited participants are connected, providing precision control of resources. In a cascaded conference, you can view participants in a tree view that displays each participant according to the conference to which each is connected.

Note   For Release 4.1, if an MP failure occurs in a cascaded conference, local Cisco IPVC 35xx MCU users can see this status in the Create Conference window or Conference Control interface. This status, however, only appears if it was the local EMP or MP that was lost. If the EMP of a slave Cisco IPVC 35xx MCU is lost, then the user of the master Cisco IPVC 35xx MCU can view which participants are without audio/video in the Participant List tab. If the EMP of the master Cisco IPVC 35xx MCU is lost, then slave Cisco IPVC 35xx MCUs do not receive any indication that there has been MP failure.

Procedure

Step 1   In the Participant List tab, invite another conference on the host Cisco IPVC 35xx MCU or on another Cisco IPVC 35xx MCU by typing the number in the **Invite #** field and clicking **Dial**.

The invited conference and connected participants appear in the host conference participant list in the Participant List tab.

Inviting Participants to a Cascaded Conference

All users can invite participants to a cascaded conference in the Advanced Invitation tab of the Conference Control interface.

Procedure

Step 1   In the Conference Control interface, click the **Advanced Invitation** tab.

Step 2   In the **MCU** column, choose the conference to which the invited participant connects upon acceptance of the conference invite.

Viewing Participants in a Cascaded Conference

In the Conference Control interface, you can view participants in a cascaded conference in a hierarchical display in one of the following two ways:

- Normal View—All conference participants appear in a single list. Cascaded participants appear without any indication of the cascadedCisco IPVC 35xx MCU connection.

- Tree View—Conference participants appear in an expandable tree view showing cascaded Cisco IPVC 35xx MCU connections to the conference. Click the plus sign (+) next to the name of the cascaded Cisco IPVC 35xx MCU to expand the tree showing cascaded conference participant details.

Procedure

Step 1   In the Participant List tab, click **Normal View** to display cascaded conference participants in a single list or **Tree View** to display conference participants in a tree view.

Terminating Conferences

In the Conference Control interface, users with Chair Control-level access can terminate a conference, which ends that conference and disconnects the participants.

Procedure

Step 1   On the control bar, click **Terminate Conference**.

Signing Out of a Conference

When you finish configuring or viewing details of the current conference, you can sign out.

Procedure

Step 1   On the control bar, click **Sign out**.

Troubleshooting the Cisco IPVC 35xx MCU

Revised: January 2006, OL-7777-03

This chapter describes the following topics:

Problems You Might Encounter Setting the IP Address

This section identifies problems that you might encounter when you assign an IP address to a new Cisco IPVC 35xx MCU, and suggests possible solutions.

Symptom I cannot access the Cisco IPVC 35xx MCU through the serial port.

Information from the Cisco IPVC 35xx MCU does not appear on the terminal emulator window.

> **Recommended Action** Make sure that the terminal emulator modem is set using the parameters as follows:
>
> - 9600 baud rate
> - 8 data bits
> - No parity
> - 1 stop bit
> - No flow control
>
> **Recommended Action** Make sure that the terminal cable that ships with the unit or a null cable is securely connected to the serial port and to the computer serial port.
>
> **Recommended Action** Verify that the Cisco IPVC 35xx MCU can communicate with the terminal.

Procedure

Step 1   Launch the terminal emulation software installed on the computer connected to the
Cisco IPVC 35xx MCU serial port.

A prompt appears.

Step 2   Press **Enter**.

If the prompt moves, the terminal emulator is communicating with the Cisco IPVC 35xx MCU.

Step 3   Restart the Cisco IPVC 35xx MCU.

A log of the startup events appears on the computer monitor.

If nothing appears, check the cable connection between the Cisco IPVC 35xx MCU and the computer.
You must use the terminal cable that ships with the unit or a null cable. If the problem persists, contact
Cisco Technical Support for assistance.

Symptom   The terminal emulator does not display the configuration menu.

Possible Cause   After the power to the Cisco IPVC 35xx MCU is turned on, the terminal emulator
connection displays two prompts that you can use to interact with the Cisco IPVC 35xx MCU. The
first prompt is "Press any key to enter debug mode." If you press any key, an interactive prompt
appears on the screen and the bootup process stops. You must restart the Cisco IPVC 35xx MCU and
wait for the second prompt to configure the IP address. The second prompt is, "Press any key to start
configuration." To restart the Cisco IPVC 35xx MCU, do one of the following actions below.

Recommended Action   Press Ctrl-X.

Recommended Action   Press the recessed RST button on the Cisco IPVC 35xx MCU front panel.

Problems You Might Encounter When You Configure the Cisco IPVC 35xx MCU

This section identifies problems that you might encounter when you configure the module and suggests
solutions.

Symptom   The Cisco IPVC 35xx MCU takes a long time to respond when I upload a configuration file.

Possible Cause   The Cisco IPVC 35xx MCU can freeze when the configuration settings you upload
require resetting.

Recommended Action   Push the reset button on the front panel of the Cisco IPVC 35xx MCU to
perform a hard reset.

About LED Indications

This section identifies problems that the LEDs can indicate, and suggests possible solutions.

Symptom   The 10/100BaseT link LED does not light up.

Possible Cause   The 10/100BaseT link LED is embedded in the 10/100BaseT jack on your left as you face the Cisco IPVC 35xx MCU front panel. When this LED is lit, it indicates that the Cisco IPVC 35xx MCU is connected to the network.

Recommended Action   Make sure that the Ethernet cable is connected to the 10/100BaseT-1 jack on the front panel of the Cisco IPVC 35xx MCU.

Recommended Action   Make sure that the devices at both ends of the link are powered-up.

Recommended Action   Make sure that you use a RJ-45 jack with standard wiring to connect the Ethernet cable to the Cisco IPVC 35xx MCU 10/100BaseT-1 jack.

Recommended Action   Reset the Cisco IPVC 35xx MCU by pressing the RST button on the front panel or by clicking **Reset** in the toolbar of the Administrator interface.

After the Cisco IPVC 35xx MCU restarts, check the link LED.

Recommended Action   Perform a ping test from a PC terminal to the Cisco IPVC 35xx MCU IP address. If the Cisco IPVC 35xx MCU is connected to the network, the ping returns the message "Reply from …". If the Cisco IPVC 35xx MCU does not respond to the ping, the ping returns the message "Request timeout."

If you receive a "Request timeout" message, try replacing the cable and repeat the ping test. Also, make sure that you properly configure the Cisco IPVC 35xx MCU IP address and subnet mask, and the router IP address.

Symptom   Why doesn't the GK Reg LED light up?

Possible Cause   The GK Reg LED indicates that the Cisco IPVC 35xx MCU has an active registration with the gatekeeper.

Recommended Action   Make sure that you specify the gatekeeper with which you want the Cisco IPVC 35xx MCU to register in the Cisco IPVC 35xx MCU Administrator interface. See the "Using the Cisco IPVC 35xx MCU Setup Wizard" section on page 2-11 for more information.

Recommended Action   Make sure that the IP address of the gatekeeper the Cisco IPVC 35xx MCU is to register with is correct.

Recommended Action   Make sure that the gatekeeper is working.

Monitoring from a Remote Site

The Administrator interface allows you to monitor Cisco IPVC 35xx MCU functions from a remote site. The LEDs are represented on the LED Monitoring tab of the Administrator interface. You can access this page from any computer on the LAN and monitor the module for connectivity or communication problems.

Procedure

Step 1   Launch a Java-based web browser.

Step 2   In the address or URL field, enter the IP address of the Cisco IPVC 35xx MCU that you want to monitor.

The Cisco IPVC 35xx MCU access window appears.

Step 3   In the **Name** field, enter a valid user name.

Step 4   In the **Password** field, enter the user password.

Step 5   Click **Go**.

The Administrator interface appears.

Step 6   On the sidebar, click **Board**.

The LED Monitoring tab appears. Table 5-1 describes the LEDs that appear on the page.

Table 5-1   LEDs on the Cisco IPVC 35xx MCU Administrator Monitoring Page

LED	Description
10/100 BaseT-1 Link	Embedded in the model-number side of the 10/100 BaseT connector. It lights green when there is connection between the Cisco IPVC 35xx MCU and network.
10/100 BaseT-1 Port Speed	Embedded in the serial-port side of the 10/100 BaseT connector. It lights green when the Ethernet connection supports 100 Mb. It is off when the Ethernet connection supports 10 Mb.
GK Reg	Lights green when the Cisco IPVC 35xx MCU has a valid registration with the gatekeeper.
CPU High	Lights green when the Cisco IPVC 35xx MCU is using more than 50% of its processing capacity.
Alarm	Lights green when the Cisco IPVC 35xx MCU requires a reset.
ACT	Lights green when one or more conferences are active on the Cisco IPVC 35xx MCU.

Using Advanced Command Line Commands

This section describes advanced command line commands that you can access through the
Cisco IPVC 35xx MCU serial port. These commands allow you to set additional module operating
parameters that are not available in the web interfaces. This following topics describe these commands:

Accessing the Command Line Commands through the Serial Port

You access command line commands through the serial port of the Cisco IPVC 35xx MCU device.

Procedure

Step 1   Connect the appropriate ends of the terminal cable to the serial port on the computer and the serial port on the Cisco IPVC 35xx MCU.

> ✎
>
> **Note**   The terminal cable is a null cable that ships with the Cisco IPVC 35xx MCU.

Step 2   Launch the terminal emulator on the computer.

Step 3   Set the communication values for the terminal emulator as follows:

- 9600 Baud rate
- 8 data bits
- 1 stop bit
- No parity
- No flow control

Step 4   After the terminal emulator session starts, press the RST button on the Cisco IPVC 35xx MCU front panel or click **Reset** in the LED Monitoring tab of the Board section in the Administrator interface.

A log of the auto-boot events appears on the computer.

Step 5   When the message "Press any key to start configuration" appears on the screen, press any key within six seconds.

- The following command line options appear.
- Enter <N> to configure default network port values
- Enter <P> to change the configuration software password
- Enter <A> to display advanced configuration menu
- Enter <Q> to quit configuration menu and start the Cisco IPVC 35xx MCU

Step 6   Select an option to execute.

Configuring the Web Server Port

This section describes how to change the web server port number. This way, you can set the port number that the Cisco IPVC 35xx MCU uses for posting its web pages. The default value is 80, which is the standard for web server ports. If another port is used in your environment, you can use this command to change the Cisco IPVC 35xx MCU web server port setting.

Procedure

Step 1   At the prompt for the command line options, press **A** to display the advanced command menu.

The Advanced command menu appears.

Step 2   At the prompt, press **1** and press **Enter** to configure the web server port.

Step 3   At the "Enter a new port number for the web server" prompt, enter the value that you want to use and press **Enter**.

The Cisco IPVC 35xx MCU uploads the configuration change and then resumes the boot cycle.

Restoring the Factory Default Settings

This section describes how to restore factory configuration settings to the Cisco IPVC 35xx MCU. Restoring these settings does not reset the IP address information.

Procedure

Step 1   At the prompt for the command line options, press **A** to display the advanced command menu.

The Advanced command menu appears.

Step 2   At the prompt, press **2** to restore the factory defaults.

Step 3   At the "Are you sure you want to restore factory configuration? [y, n]" prompt, enter **y** and press **Enter**.

Factory default settings are restored.

Configuring the Ethernet Port

This section describes how to set the Ethernet speed and duplex that the Cisco IPVC 35xx MCU uses.

Procedure

Step 1   At the prompt for the command line options, press **A** to display the advanced command menu.

The Advanced command menu appears.

Step 2   At the prompt, press **3** to change the network working mode.

A list of Ethernet configuration options appear.

Step 3   At the prompt, select one of the following options:

- Press **1** to set the Ethernet port for 10 MBs half-duplex operation.

- Press **2** to set the Ethernet port for 100 MBs half-duplex operation.

- Press **3** to set the Ethernet port for 10 MBs full-duplex operation.

- Press **4** to set the Ethernet port for 100 MBs full-duplex operation.

- Press **5** to set the Ethernet port to Auto so that the Cisco IPVC 35xx MCU negotiates the port setting with the router or switch. This is the default setting.

- Press any other key to return to the configuration menu without changing the setting.

Step 4   Press **Enter**.

The Cisco IPVC 35xx MCU uploads the configuration and restarts the boot cycle.

About Bandwidth Considerations

The amount of bandwidth required during a conference depends on a number of factors, including whether all participants are connected only through an IP network or also to other networks.

The following factors affect the available bandwidth when all the conference participants connect to the IP network:

- The capacity of the video conferencing terminal application (endpoint) in use.

- Whether or not audio transcoding is in use.

- System policies set by the system administrator.

The following factors affect the available bandwidth when one or more of the conference participants is connected to the conference through a gateway:

- The gateway connection

- The gateway audio transcoding capabilities