



Troubleshooting Guide for Cisco Unified Videoconferencing 3500 MCU Release 5.1

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-12051-01



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 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.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, 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, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, 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. (0609R)



Preface	v
Purpose	v
Audience	v
Document Conventions	v
Obtaining Documentation	vi
Cisco.com	vi
Product Documentation DVD	vi
Ordering Documentation	vi
Documentation Feedback	vii
Cisco Product Security Overview	vii
Reporting Security Problems in Cisco Products	vii
Product Alerts and Field Notices	viii
Obtaining Technical Assistance	viii
Cisco Technical Support & Documentation Website	viii
Submitting a Service Request	ix
Definitions of Service Request Severity	ix
Obtaining Additional Publications and Information	x

CHAPTER 1

Troubleshooting the Cisco Unified Videoconferencing 3500 MCU	1-1
Resolving MCU Failure to Register with the Gatekeeper	1-2
Resolving Front Panel LED Issues	1-2
Resolving MCU Conference Initiation Failure	1-3
Resolving Conference Access Failure	1-4
Resolving Cascading Failure	1-4
Resolving Quality Issues in Cascaded Conferences	1-5
Resolving Endpoint Disconnection Issues	1-5
Resolving Unexpected Conference Termination	1-5
Resolving Presentation Issues	1-6
Resolving Participant Connection Issues	1-6
Resolving Unexpected SIP Call Disconnection	1-6
Resolving Audio and Video Issues in SIP Calls	1-6



Preface

Revised: November 27, 2006, OL-12051-01

Purpose

This guide provides the information you need to troubleshoot problems in the Cisco Unified Videoconferencing 3500 MCU.

Audience

This guide is intended for network administrators and end users who need help addressing operational problems in the Cisco Unified Videoconferencing 3500 MCU.

Document Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in boldface .
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .
[]	Elements in square brackets are optional.
{ x y z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in <code>screen font</code> .
boldface screen font	Information you must enter is in boldface screen font .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .

Convention	Description
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

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 library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

If you do not have a user ID or password, you can register at this URL:

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

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

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 do the following:

- 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 encryption key 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 to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: <http://tools.cisco.com/RPF/register/register.do>) Registered users can access the tool at this URL: <http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

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 Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and

pastings **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.

**Tip**

Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

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 Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:
<http://www.cisco.com/offer/subscribe>
- 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 channel product 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>
- *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 where networking professionals 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>
- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:
<http://www.cisco.com/univercd/cc/td/doc/abtnicd/136957.htm>

- 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>



Troubleshooting the Cisco Unified Videoconferencing 3500 MCU

This section covers problems you might encounter when configuring, operating and managing the Cisco Unified Videoconferencing 3500 MCU. This chapter provides suggested actions you can use to solve the problems, and includes the following topics.

This section describes the following topics:

- [Resolving MCU Failure to Register with the Gatekeeper, page 1-2](#)
- [Resolving Front Panel LED Issues, page 1-2](#)
- [Resolving MCU Conference Initiation Failure, page 1-3](#)
- [Resolving Conference Access Failure, page 1-4](#)
- [Resolving Cascading Failure, page 1-4](#)
- [Resolving Quality Issues in Cascaded Conferences, page 1-5](#)
- [Resolving Endpoint Disconnection Issues, page 1-5](#)
- [Resolving Unexpected Conference Termination, page 1-5](#)
- [Resolving Presentation Issues, page 1-6](#)
- [Resolving Participant Connection Issues, page 1-6](#)
- [Resolving Unexpected SIP Call Disconnection, page 1-6](#)
- [Resolving Audio and Video Issues in SIP Calls, page 1-6](#)

Resolving MCU Failure to Register with the Gatekeeper

This section describes what to do if the MCU fails to register with the Cisco IOS H.323 Gatekeeper.

Possible Causes	Verification Steps
The gatekeeper address is set incorrectly.	Verify the Gatekeeper IP address settings.
TCP/IP setup issue.	<ul style="list-style-type: none"> Verify that the MCU is assigned a unique IP address. Verify that the subnet mask and default gateway subnet mask are set correctly.
LAN or cable problem	<ul style="list-style-type: none"> Verify the switch port settings. Verify that the Ethernet cable is straight through. Try another Ethernet cable.
The MCU cannot register to a Cisco MCM. The Cisco MCM may not understand the syntax of the label "MCU".	Change the registration name of the MCU to "GW" in the MCU Advanced Commands window.

Resolving Front Panel LED Issues

This section describes what to do if MCU module front panel LEDs are off at all times, including during the power off, power on cycle.

Possible Causes	Verification Steps
Power supply problem	<ul style="list-style-type: none"> Make sure that the power supply LED is green. Check the AC cable and fuse.
The MCU module is not inserted correctly in the Cisco Unified Videoconferencing 3545 chassis, or a back plane pin is bent.	<ul style="list-style-type: none"> Open the telecom latch screws and extract the MCU module from its slot. Verify that there are no bent pins on the back plane (using a flashlight, if necessary). Re-insert the MCU module carefully closing the latches.

Resolving MCU Conference Initiation Failure

This section describes what to do if MCU conference initiation fails.

Possible Causes	Verification Steps
The MCU is set to work with an external authorization server, but no authorization server is configured.	Verify that the External conference authorization policy option is set to None in in MCU > Settings > Advanced.
The MCU is set to work with an external authorization server, but the authorization server is not configured properly to work with the MCU.	Verify that the MCU IP address is correctly configured in the authorization server.
The MCU is set to prevent endpoints from creating conferences.	Verify that the Conferences can be created using option is set to Scheduler, Web, Control API and dial-in in MCU > Settings > Advanced.
There are not enough MCU resources available for the desired conference.	<ul style="list-style-type: none"> Verify that the service you are using reserves the minimum number of parties (2) and allows expansion up to the required number of parties. Verify that current calls are not utilizing all resources by check the available MCU capacity and then trying to disconnect other calls in order to find the problem.
The service requires one EMP video processor, but no EMP module appears to be registered with the MCU.	<ul style="list-style-type: none"> Ping the EMP module. Open a Telnet connection to the IP address of the required EMP module. Open a serial connection to the EMP module if there is no response from the IP address. Type the advanced command <code>modifyTargetDevice</code> to ensure that the EMP is configured to work with the correct MCU. <p>You can perform this operation using the serial connection via the countdown menu visible after rebooting the EMP.</p> <ul style="list-style-type: none"> Reboot the EMP after modifying the controlling MCU.

Resolving Conference Access Failure

This section describes what to do if an endpoint cannot be invited to a conference or dial into the conference.

Possible Causes	Verification Steps
The MCU is configured to work with an authorization server, but the endpoint is not authorized and therefore the authorization server rejects the call.	Check if the endpoint is authorized in the authorization server.
The endpoint is currently in a call.	Confirm that the endpoint is not busy/in a call.
There are not enough MCU resources available for the desired conference.	Remove one of the current participants to verify that the endpoint can join successfully.

Resolving Cascading Failure

This section describes what to do if MCU conference cascading fails.

Possible Causes	Verification Steps
The invited conference does not exist, and the remote MCU is not in Ad Hoc (Scheduler, Web, Control API and dial-in) mode.	<ul style="list-style-type: none"> Using the remote MCU web interface, verify that the remote conference exists or that the Conferences can be created using option is set to Scheduler, Web, Control API and dial-in in MCU > Settings > Advanced. If ad hoc conferencing is not allowed for the remote MCU, and the remote conference does not exist, create the conference and then cascade it (web/dial invite).
Service prefixes are not unique and there is service prefix conflict.	Verify that all cascaded MCU modules have unique service prefixes.
The remote MCU module is not registered with its gatekeeper.	Verify proper registration of all MCU modules with their respective gatekeepers.
Not enough ports are available to accomplish cascading. Note Cascading requires one port from each conference.	Check that the number of free ports on each EMP used is not zero.
Services are not synchronized.	Verify that service definitions do not include differences such as H.235 being enabled on one conference only.

Resolving Quality Issues in Cascaded Conferences

This section describes what to do if a cascaded conference suffers long delays or bad lip synchronization.

Possible Causes	Verification Steps
Unsuitable topology used (for example, chain topology used unnecessarily).	<ul style="list-style-type: none"> • One single central MCU should invite all other cascaded MCUs. • We recommend that you do not have more than one level of cascaded MCUs. • Use a star topology, where the central MCU is in the center of the star, and other cascaded MCU modules are on the arms of the star.

Resolving Endpoint Disconnection Issues

This section describes what to do if endpoints unexpectedly drop out of the MCU conference.

Possible Causes	Verification Steps
Unreliable network link.	Check network link quality (round trip time should be less than 300 msec).

Resolving Unexpected Conference Termination

This section describes what to do if a conference on the MCU unexpectedly terminates.

Possible Causes	Verification Steps
The Ad hoc conferences terminate when option in MCU > Settings > Advanced is set to Conference creator leaves and the conference creator has left the conference.	Set the Ad hoc conferences terminate when option in MCU > Settings > Advanced to Last participant leaves.
Unreliable network link between the MCU and the gatekeeper.	Check network link quality (round trip time should be less than 300 msec).

Resolving Presentation Issues

This section describes what to do if you cannot start or receive a presentation during a conference.

Possible Causes	Verification Steps
H.239 functionality is not enabled on your endpoint.	<ul style="list-style-type: none"> Verify that H.239 is enabled on the endpoint. Make a point-to-point call to another endpoint and verify that you can start a presentation.
Presentation is not configured in the MCU service used in your conference.	Configure the service to support presentation in MCU > Services.
MCU presentation definitions in the service are not supported by your endpoint (frame rate, frame size, codec).	Check that your endpoint supports the frame size, frame rate and video codec as defined in the service.

Resolving Participant Connection Issues

This section describes what to do if you have difficulty connecting 96 participants in a conference even though there are enough MVP resources available.

Possible Causes	Verification Steps
The MCU is configured to support DTMF detection during the call. Note DTMF detection reduces the number of supported audio ports from 96 to 72.	Disable DTMF detection via the advanced commands.

Resolving Unexpected SIP Call Disconnection

This section describes what to do if a SIP call unexpectedly disconnects after 30 seconds.

Possible Causes	Verification Steps
DNS is not fully configured on the MCU and user agents.	Verify that DNS is configured on user agent and MCU.

Resolving Audio and Video Issues in SIP Calls

This section describes what to do if audio or video channels in SIP calls do not open.

Possible Causes	Verification Steps
The MCU does not publish all its capabilities when inviting other participants.	Check the Use Empty Invite when sending invite messages to endpoints option in MCU > Protocols > SIP > Advanced.