



Release Notes for Cisco Unified Videoconferencing Gateway 3500 Release 5.0

Revised: May 15, 2006 OL-10588-01

These release notes describe the new features and caveats for Cisco Unified Videoconferencing Gateway 3500 Release 5.0 for the following Cisco products:

- Cisco Unified Videoconferencing 3527 PRI Gateway
- Cisco Unified Videoconferencing 3522 BRI Gateway
- Cisco Unified Videoconferencing 3545 PRI Gateway
- Cisco Unified Videoconferencing 3545 Serial Gateway

Use these release notes with *Administrator Guide for Cisco Unified Videoconferencing 3527 PRI Gateway and 3522 BRI Gateway Release 5.0* and *Administrator Guide for Cisco Unified Videoconferencing 3545 PRI Gateway and 3545 Serial Gateway Release 5.0*.



Note

In this document, these products are referred to as Cisco Unified Videoconferencing Gateway 3500 unless otherwise noted.



Note

To view the release notes for previous versions of Cisco Unified Videoconferencing Gateway 3500, go to: http://cisco.com/en/US/products/hw/video/ps1870/prod_release_notes_list.html

You can access the latest software upgrades and release notes for all versions of Cisco Unified Videoconferencing Gateway 3500 on Cisco Connection Online (CCO) at the following URL:

<http://cisco.com/kobayashi/sw-center/sw-video.shtml>

Contents

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New and Changed Information, page 2](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© <year> Cisco Systems, Inc. All rights reserved.

- [Caveats for Cisco Unified Videoconferencing Gateway 3500 Release 5.0, page 3](#)
- [Obtaining Documentation, page 5](#)
- [Documentation Feedback, page 6](#)
- [Cisco Product Security Overview, page 6](#)
- [Obtaining Technical Assistance, page 7](#)
- [Obtaining Additional Publications and Information, page 9](#)

Introduction

The Cisco Unified Videoconferencing Gateway 3500 enables audio, video and data communication between H.320 endpoints that connect through Integrated Services Digital Network (ISDN), and H.323 endpoints that connect through a packet-based network. For voice-over-IP, the gateway enables Public Switched Telephone Network (PSTN) voice callers to connect with IP voice callers.

System Requirements

This section includes the following topics:

- [Supported Upgrades, page 2](#)

Supported Upgrades

You can upgrade directly from Cisco Unified Videoconferencing Gateway 3500 Release 4.x to Release 5.0.

New and Changed Information

All Cisco Unified Videoconferencing Gateway 3500 products include the following new features:

- H.243 support
- IVR Operator digit
- Support for 1344 Kbps and 1536 Kbps bit rates

The Cisco Unified Videoconferencing 3545 Serial Gateway includes the following additional new features:

- Support for the H.239 standard
- Support for the H.264 advanced video codec
- Media encryption (H.235 v3.0)
- Peer-to-peer dialing
- Factory defaults reset via Web, SNMP and CLI
- Notification when Ethernet is not 100 full-duplex
- Common administrator user name and password for web and Telnet/FTP access

- Date and time on operator log files
- Operator and Read-only user types are added to the already existing Administrator user type
 - Operator—Has read-only access to the whole of the Gateway web user interface, and can monitor and disconnect calls
 - Read only—Has read-only access to the whole of the Gateway web user interface, but cannot modify any Gateway settings
- Additional SNMP traps:
 - Call is out of synchronization
 - Serial cable mismatch

Caveats for Cisco Unified Videoconferencing Gateway 3500 Release 5.0

This section includes the following topics:

- [Resolved Caveats for Cisco Unified Videoconferencing Gateway 3500 Release 5.0, page 3](#)
- [Open Caveats for Cisco Unified Videoconferencing Gateway 3500 Release 5.0, page 3](#)

Resolved Caveats for Cisco Unified Videoconferencing Gateway 3500 Release 5.0

The following issues have been resolved since Release 4.0:

- The web user interface correctly displays the Gateway location or IP address.
- When using the improved G.722.1, H.264 and H.239 capability policy, these capabilities are not published to the ISDN or to the IP legs to prevent some legacy equipment crashing.
- 2*B calls via the Gateway operate correctly.
- Interoperability with the Cisco IPVC 35xx MCU for calls using G.728 at 128 Kbps.
- Improved interoperability with ISDN Polycom VSX version 7.5.2.
- Improved clearing cause is sent to the IP endpoint in some cases.

Open Caveats for Cisco Unified Videoconferencing Gateway 3500 Release 5.0

This section lists possible unexpected behaviors by Cisco Unified Videoconferencing Gateway 3500 Release 5.0 and is sorted by gateway product.

All Cisco Unified Videoconferencing Gateway 3500 Products

- Upgrade/downgrade problems may occur due to lack of memory. If the “Upgrade process failed: The uploaded file size is larger than the maximum available memory” message displays in the Upgrade Utility, manually reboot the board and retry the upgrade.

- When using TANDBERG 1500 MXP on the IP side, it may take about 20 seconds for the video channel to open from the MXP to the Gateway.
- The start of the IVR message is missing in calls from an ISDN Polycom VSX endpoint.
- H.239 interoperability issues may occur when working with eConf.
- H.239 interoperability issues occur in calls between a TANDBERG ISDN 990MXP endpoint and a Polycom VSX LAN endpoint.
- H.235 interoperability issues may occur when working with a TANDBERG 4.1 endpoint. The audio channel from the endpoint via the Gateway may fail to open as an encrypted channel. In such cases, the Gateway will disconnect the call.
- H.239 supports only the H.263 codec in the second video channel. H.264 is not supported.
- We recommend that you use an MVP when working with the MCU in H.239 mode.
- When working in Peer-to-Peer mode, the front Gatekeeper (GK) LED is always lit.
- Video may freeze in calls between ISDN Polycom FX and IP TANDBERG MXP.

Cisco Unified Videoconferencing 3527 PRI Gateway, 3522 BRI Gateway and 3545 PRI Gateway

- Difficulties may occur when using Fast Start. We recommend that you do not activate Fast Start.
- H.239 is not supported in 2*B calls.

Cisco Unified Videoconferencing 3545 Serial Gateway

- Connection problems occur in IP-to-IP calls via two Serial Gateways using Polycom VSX 7000.

Troubleshooting

- We recommend that you use Microsoft Explorer version 5.0 or later as your browser.
- Interoperability issues may occur with Aethra Maia384 on the ISDN. Solve the problem by sending the ChangeBondingCID advanced command with the parameter value “enable” to the Gateway.
- Calls may fail when using TANDBERG endpoints on the ISDN with the bit rate set to “Auto”. Solve the problem by sending the ClearBondXflag advanced command with the parameter value “enable” to the Gateway.
- When making a 128 Kbps call from an ISDN Sony PCS-1, H.239 may not open correctly. Increasing the call bit rate solves this issue.
- H.239 interoperability issues may occur when working with Aethra endpoints on the ISDN when making a TCS4 or IVR call. Solve this issue by sending the SimulateVideoOff advanced command with the parameter value “enable”.
- When working with VSX300 on the ISDN side, if using G.722.1 with H.263, there will be no video seen in the VSX. Disable the G.722.1 in the GW media modes in order to solve this issue.
- When using G.722.1 with H.263, video is lost on a Polycom VSX300 ISDN endpoint. Solve this problem by disabling G.722.1 in the Media Modes section of the Gateway Settings tab.
- Opening an H.239 channel to a TANDBERG MXP on the ISDN side may fail. Simply retry and the channel will open successfully.

For additional troubleshooting information, see the Troubleshooting chapter in the *Administrator Guide for Cisco IPVC-3527-GW1P and Cisco IPVC-3522-GW4B Release 5.0* and *Administrator Guide for Cisco IPVC-3545-GW2P and Cisco IPVC-3545-GW4S Release 5.0* at the following URL:

http://cisco.com/en/US/products/hw/video/ps1870/prod_maintenance_guides_list.html

Related Documentation

For administration documentation, see the *Administrator Guide for Cisco Unified Videoconferencing 3527 PRI Gateway and 3522 BRI Gateway Release 5.0* and *Administrator Guide for Cisco Unified Videoconferencing 3545 PRI Gateway and 3545 Serial Gateway Release 5.0* at the following URL:

http://cisco.com/en/US/products/hw/video/ps1870/prod_maintenance_guides_list.html

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



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>

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCVP, the Cisco logo, and Welcome to the Human Network 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, 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, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, 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. (0711R)

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.

© 2006 Cisco Systems, Inc. All rights reserved.