Avaya Branch Gateways 5.2.1 Version 30.27.1 (G250, G350, G450,G700,TGM550) Version 30.27.2 (G430 only) Release Notes

Issue 1
September 9, 2013

Contents

© 2013 Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product, while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com.

Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by the said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License type(s)

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processor up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than a single instance of the same database.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User” means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

Certain software programs or portions thereof included in the Software may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those product that have distributed Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/ThirdPartyLicense/

You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

“Toll fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud Intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

"Avaya" and "Avaya Aura" are the registered trademarks of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and "Linux**"** is a registered trademark of Linus Torvalds.

Downloading documents

For the most current versions of documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product.

For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Changes Delivered to Branch Gateways 5.2.1

Branch Gateways 5.2.1 Release Notes

Branch Gateway firmware releases and versions are cumulative. Branch Gateways 5.2.1 includes the following Branch Gateway firmware versions:

- 30.27.2
- 30.27.1
- 30.26.0
- 30.24.0
- 30.21.0
- 30.20.1
- 30.19.0
- 30.18.1
- 30.17.x
- 30.16.0
- 30.15.0
- 30.14.0
- 30.13.2
- 30.12.1
- 30.10.4

The changes delivered to Branch Gateways 5.2.1 are grouped as follows:

Product Support Notices

Some problems are also documented as Product Support Notices (PSN). The PSN number defines the related document and appears in the Problem column in the tables.

To read the PSN description online:

1. Go to the Avaya support site at http://support.avaya.com.
2. Click **Product Notices**.
3. Click **Product Support Notices**.
4. Type the last four digits of the PSN number into your web browser's "Find on Page" function to search the page for a link to the PSN.
5. Click the PSN title link to open the PSN.

Problems Fixed in Branch Gateways 5.2.1 Version 30.27.2

Important:
Version 30.27.1 is applicable only to G250, G350, G450, G700, and TM550 Branch Gateways.

Version 30.27.2 is applicable only to G430 Branch Gateway and includes all fixes in 30.27.1.

The following fixes were delivered to Branch Gateways 5.2.1**.**

Table 1: Fixes delivered to Branch Gateways 5.2.1 Version 30.27.2

Problem	Keywords	Workaround (for prior versions)
G430 G430 did not send all the supported traps.	130100	

Problems Fixed in Branch Gateways 5.2.1 Version 30.27.1

Important:
Version 30.27.1 is applicable only to G250, G350, G450, G700, and TM550 Branch Gateways.

Version 30.27.2 is applicable only to G430 Branch Gateway and includes all fixes in 30.27.1.

The following fixes were delivered to Branch Gateways 5.2.1**.**

Table 2: Fixes delivered to Branch Gateways 5.2.1 Version 30.27.1 ***1 of 2***

Problem	Keywords	Workaround (for prior versions)
G430 Raise a trap or an alarm when a FAN failure occurs in EM200.	120290	
G430, G450 DSP Core failure occurred when the output buffer of the Echo Canceller was exceeded.	130068	

Table 2: Fixes delivered to Branch Gateways 5.2.1 Version 30.27.1 *2 of 2*

Problem	Keywords	Workaround (for prior versions)
G430, G450 The system randomly displayed the hostname when the **`show running-config`** CLI command was run.	130034	
G350 Gateway did not register to Communication Manager after S8300 rebooted.	120233	
G430, G450 The **`show platform main`** CLI command no longer displays information about SODIMM Memory Socket #2 in new gateways that have only one socket.	120251	
G430, G450 After a system reset, some gateways that had more than one controller listed in the MGC list did not successfully register with the first entry in the list.	120260	
G430, G450, G350, G250, G700, TGM550 MM710B was not updated when the Restore operation was performed.	120263	
G430, G450, G350, G250, G700, TGM550 Increase the uptime duration displayed by the **`show system`** CLI command so that it rolls over only once every 497 days.	120284	
G450 DSP gain/loss is no longer applied the re-generated DTMF digits from RTP telephony events and the default level has been increased by 3dB. The change in transmitted DTMF level from previous release can range from -3 to +9 depending on the country code administered in Communication Manager.	120298	

Known Problems in Branch Gateways 5.2.1 Version 30.27.1 and Version 30.27.2

This release includes the following known issues in Branch Gateways 5.2.1.

Table 3: Known problems in Branch Gateways 5.2.1 Version 30.27.1 and Version 30.27.2

Problem	Keywords	Workaround
G450 If STP (Spanning Tree Protocol) is not configured uniformly, the G450 might not register with the primary Communication Manager Server after a reset.	090595	This behavior is normal. Enable or disable STP on both the G450 LAN port and the peer device connected to G450 LAN port.
G450 Enabling RTCP causes DSP Core failure if more than 20 traceroute hops are encountered.	130043	Disable RTCP

Changes Delivered to Previous Branch Gateways 5.2.1 Versions

Problems Fixed in Branch Gateways 5.2.1 Version 30.26.0

Note:
Version 30.22.0 is no longer available on the Avaya support site. However, all the fixed problems from release 30.22.0 are included in the current release 30.26.0.

The following fixes were delivered to Branch Gateways 5.2.1**.**

Table 4: Fixes delivered to Branch Gateways 5.2.1 Version 30.26.0 ***1 of 4***

Problem	Keywords	Workaround (for prior versions)
G430,G450 To help improve system stability memory error correction (ECC) is added and signal timing for DDR memory is adjusted.	120271 120285	
G450 In some configurations when the G450 gateway cannot register to a controller for longer than the total search time, some media modules may enter an initializing state that clears only after the gateway registers again.	110232	
G430,G450 A counter tracks the number of active traceroutes that are used in monitoring VoIP activity. When the counter does not function correctly, new traceroutes are not generated and the event log is filled with errors.	110341	

Table 4: Fixes delivered to Branch Gateways 5.2.1 Version 30.26.0 ***2 of 4***

Problem	Keywords	Workaround (for prior versions)
G430,G450 ASG users are asked to enter a new password whenever they log into the gateway. The system continues to request a new password even after the user provides one.	120052	1. Use SSH to log into gateway as root user. 2. Enter valid password for root user, or use fake password "123456". If the fake password is used, abort the login attempt after the password is entered once. If a valid password is used, exit from the SSH session
G430,G450 With a mix of modem, fax, and voice traffic, MP20 may not function correctly	120066	
G430,G450 Network traffic that is beyond normal capacity, such as denial of service attacks, hinders the mechanism that monitors the condition of VoIP DSPs. This change brings the DSPs back into service faster.	120224	
G430,G450 When silence suppression is enabled, RTP transmitters encode only marker bits.	120236	
G430,G450 When the system moves into the pass-through mode, there is a jump in sequence number. This issue is now resolved.	100293	
G430,G450 A new VoIP parameter "53" has been added. This parameter is used to combat the negative effect of the long echo paths on T.38 or Avaya relay fax relay	110252	
G450 After boot-up, a DSP slot is reset. The slot either does not contain a DSP or contains an unsupported DSP. The reset of the DSP slot tries to boot the DSP. This change ensures that the slot retains the correct state. This is an issue only with MP160 in a gateway with a firmware version that does not support the gateway.	110312	

Table 4: Fixes delivered to Branch Gateways 5.2.1 Version 30.26.0 ***3 of 4***

Problem	Keywords	Workaround (for prior versions)
G430,G450 The T.38 fax relay state machine operation that is used for providing robustness to third-party fax server timing is improved.	120037	
G430,G450 If DHCP option strings are used in the configuration file, the CLI prompt corrupts the DHCP offer to the phones.	120080	
G430,G450 The modem pass-through issue that was causing modem sessions to drop is resolved.	120124	
G430,G450 The modem pass-through issue that was preventing successful start-up of a modem session is resolved.	120142	
G430,G450 There is voice distortion for some country codes when signal levels are high. This issue is now resolved.	120202	
G430,G450 Sometimes, the system resets when both the processes that are used for traceroute free the same memory. Protection is added to ensure that only one process frees the memory.	120157	
G450 After a power outage or hardware reset, G450 hardware vintage 2 will automatically detect if the CPU frequency is lower than normal and correct this condition by doing software reset.	120153	Restart the gateway when the condition is detected.
G430,G450 The echo canceller is not enabled when an announcement is played on an analog trunk and the only listener is the tone detector. Echo from the playback of the announcement file triggers false tone detections.	120181	
G430,G450 The count for transmitted packets between RTCP reports is incorrectly calculated. Thus, Sender Reports are not sent.	120199	

Table 4: Fixes delivered to Branch Gateways 5.2.1 Version 30.26.0 ***4 of 4***

Problem	Keywords	Workaround (for prior versions)
G430,G450 The gateway resets when a software image is downloaded by using a freeware TFTP server for windows.	110180	
G430, G450 In some country codes, the DSP gain for talk and listen path is not always correct. This does not affect US, ETSI or TIA settings. Settings are now corrected for gateways programmed to operate with the following country codes, users might hear a slight volume change: Belgium (6), France (12), Germany (13), Netherlands (5), Nordic (24), S. Africa (25), Spain (11), and UK (10).	110263	
G430, G450 Incorrectly formatted fax relay packets can generate DSP exception.	110336	
G430, G450 RTCP packets contain the IP address of the source. When the gateway IP address has a 0 as one of the four bytes, such as 172.16.0.200, the RTCP packet shows an address of 172.16..200. The address will now be correct.	110276	
G430 Loads 30.20.0 and 30.20.1 disabled support for the MM721 media module on the G430 gateway, but the board appeared to be in service and the ISDN layer 2 remained in the establish state. This is corrected in 30.21.0.	10334	

Problems Fixed in Branch Gateways 5.2.1 Version 30.24.0

The following fixes were delivered to **Branch Gateways 5.2.1 Version 30.24.0.**

Table 5: Fixes delivered to Branch Gateways 5.2.1 Version 30.24.0

Problem	Keywords	Workaround
G250,G350,IG550 A counter that used to keep track of the number of active traceroutes used in monitoring VoIP activity did not function properly, and new traceroutes could not be generated and the event log was filled with errors.	110341	
G250 Improved voip-engine recovery upon DSP out-of-service condition.	110342	

Problems Fixed in Branch Gateways 5.2.1 Version 30.21.0

The following fixes were delivered to **Branch Gateways 5.2.1 Version 30.21.0.**

Table 6: Fixes delivered to Branch Gateways 5.2.1 Version 30.21.0

Problem	Keywords	Workaround
G250, G350 When a dsp was detected as faulty, it could not be put back into service. Now, as long as the DSP can be rebooted successfully it will be put back into service.	110317	
G700 After a G700 registers to an LSP it will only try to auto fallback to the first entry in the MGC list.	110304	

Problems Fixed in Branch Gateways 5.2.1 Version 30.20.1

The following fixes were delivered to **Branch Gateways 5.2.1 Version 30.20.1.**

Table 7: Fixes delivered to Branch Gateways 5.2.1 Version 30.20.1

Problem	Keywords	Workaround
G430, G450 During high volume fax and/or modem VoIP traffic (pass-thru or relay), a memory leak could occur. This leak would gradually prevent users from making VoIP calls.	110264	

Problems Fixed in Branch Gateways 5.2.1 Version 30.20.0

The following fixes were delivered to **Branch Gateways 5.2.1 Version 30.20.0.**

Table 8: Fixes delivered to Branch Gateways 5.2.1 Version 30.20.0

Problem	Keywords	Workaround
G450, G430 An inconsistency between some fast path tables lead to memory leak and excessive CPU utilization.	110179	
G450, G430 The sequence number did not change after sending DTMF in RTP.	110103	
G430, G450 An address variable was corrupted in the PCD code.	110218	
G430, G450 Fixed an issue with incorrect OIDs in ISDN traps.	110194	

Problems Fixed in Branch Gateways 5.2.1 Version 30.19.0

The following fixes were delivered to **Branch Gateways 5.2.1 Version 30.19.0**

Table 9: Fixes delivered to Branch Gateways 5.2.1 Version 30.19.0

Problem	Keywords	Workaround
G430, G450 Communication Manager did not receive notification of the ETR state of the MM714B, even though ETR and the MM714B were functioning properly.	110084	
G450 In extremely rare cases, an internal timeout of one of the media module tasks could cause a G450 to reset.	110162	
G430, G450 In a rare cases, during abnormal, extreme ISDN traffic, a problem with the PKINT buffer allocation scheme could cause an ISDN trunk to enter an unrecoverable failure condition.	110163	
G430, G450 You could not set SLS media Module type to MM721 while using SNMP that was set on the SLS Slot Configuration table.	110112	

Problems Fixed in Branch Gateways 5.2.1 Version 30.18.1

The following fixes were delivered to **Branch Gateways 5.2.1 Version 30.18.1.**

Table 10: Fixes delivered to Branch Gateways 5.2.1 Version 30.18.1 ***1 of 3***

Problem	Keywords	Workaround
G430, G450 After upgrading to a newer release, the following error was displayed upon start-up: ’“Failed Testing Line xxx in startup-config file: “set sync interface primary v0”’	100679	

Table 10: Fixes delivered to Branch Gateways 5.2.1 Version 30.18.1 ***2 of 3***

Problem	Keywords	Workaround
G450 The traceroute function uses udp ports whose range is spread out. In G450 Branch Gateways, the ports are spread out far enough that the range requested for use may be invalid and the traceroute will not be performed. This results in no traceroute data being reported for some ports.	101067	
G430, G450 MM721 modules in excess of the Branch Gateway limit will be alarmed as an invalid configuration and the MM ALM LED will be lit.	110018	
G430, G450 In an ESS configuration, if the Branch Gateways fail over to the ESS, all Branch Gateways will be allowed to register to the ESS if it is available.	110019	
G450 G450 incorrectly reported to CM that it supported Clock Sync over IP (CSoIP) in release 5.2.1, when in fact the feature is not actually introduced until release 6.1.	110043	
G430, G450 The talk-path could be lost when receiving RTP media from a Nortel CS1000	110049	
G430, G450 Heavy traffic can cause the MP80 to crash.	110065	
G430, G450 In rare cases the ISDN trunk can lock-up because of internal buffers overflow requiring a Branch Gateway reset. This version increases the buffers and will avoid entering in the state that causes the lock-up.	110066	
G430, G450 During a failure of the primary server, the Branch Gateway will try to register to a secondary server. If the secondary is available and responding to the Branch Gateway, the Branch Gateway should continue to try to register to it and not move on to an LSP or SLS.	100630	

Table 10: Fixes delivered to Branch Gateways 5.2.1 Version 30.18.1 ***3 of 3***

Problem	Keywords	Workaround
G430, G450 In some instances where the DS1 is being reset via Communication Manager, it could get into a state where it is no longer recognized by Communication Manager after the reset is complete.	101054	

Enhancements to Branch Gateways 5.2.1 Version 30.17.x

- Increased maximum members in an H.248 context to 128 to support larger paging groups.
- Improved VoIP performance.

MM721 ISDN Media Module

The MM721 replaces the MM720.

The MM721 Basic Rate Interface (BRI) media module contains eight ports. You can administer these ports either as BRI trunk or BRI endpoint connections, such as a telephone and data module.

Note:
If you replace the MM720 media module, first uninstall the MM720 media module before installing the MM721 media module.

For information on new features and significant enhancements in Branch Gateways 6.1, see *Avaya Aura™ Communication Manager Change Description for Release 6.0* on http://support.avaya.com.

Problems Fixed in Branch Gateways 5.2.1 Version 30.17.x

The following fixes were delivered to Branch Gateways 5.2.1**.**

Table 11: Fixes delivered to Branch Gateways 5.2.1 Version 30.17.x

Problem	Keywords	Workaround
G430, G450 During a failure of the primary server, the Branch Gateway will try to register to a secondary server. If the secondary is available and responding to the Branch Gateway, the Branch Gateway should continue to try to register to it and not move on to an LSP or SLS.	100630	
G430, G450 In some instances where the DS1 is being reset via Communication Manager, it could get into a state where it is no longer recognized by Communication Manager after the reset is complete.	101054	
G430, G450 A new echo canceller has been added to the MP-80 DSP which includes a new modem pass-through voip-parameter option (id 34, value 0x19C461) which is specifically intended to improve modem pass-thru performance over analog trunks for secure phones (STEs). Note that this change only applies to the MP-80 DSP.	100177	

Problems Fixed in Branch Gateways 5.2.1 Version 30.16.0

The following fixes were delivered to Branch Gateways 5.2.1 Version 30.16.0.

Table 12: Fixes delivered to Branch Gateways 5.2.1 Version 30.16.0 ***1 of 2***

Problem	Keywords	Workaround
G430, G450 High CPU utilization was observed when the rtcp-stat-service or rtpmon is enabled	100863	

Table 12: Fixes delivered to Branch Gateways 5.2.1 Version 30.16.0 ***2 of 2***

Problem	Keywords	Workaround
G430, G450 A new voip parameter, 93, has been added which when programmed to a value of zero, helps with duplicate digit problems that are caused by other vendor's rfc2833 leakage. You can use the new voip parameter alone or in conjunction with the existing DTMF stripping voip parameter 60.	100451.01	
G450 On first boot or after returning to factory defaults, the default password must be changed. When you opened a new SSH session from the Services port (after the default password has been changed from the Console port), you were required to enter a new password and to change the default one, although you already changed it.	100874.00	
G450 2.x The 'system show cs' CLI command did not present the correct PLDs version.	100875.00	
G430, G450 No SNMP trap was sent when a VoIP DSP went into a fault state.	100935.00	
G430, G450 When uploading an announcement file from a Media Gateway platform to a SSH server through the SCP protocol, the transfer never ended.	100880	
G430, G450 In cases where multiple calls went to the same ip address, such as ip trunking, rtp-stat-service may have shown incorrect traceroute data.	100769.00	

Problems Fixed in Media Gateways 5.2.1 Version 30.15.0

The following fixes were delivered to **Media Gateways 5.2.1 Version 30.15.0.**

Table 13: Fixes delivered to Media Gateways 5.2.1 Version 30.15.0 ***1 of 2***

Problem	Keywords	Workaround
G430 When a Multitech Modem **MT5634ZBA-USB** was connected to a USB port 1 and a USB flash disk to USB port 2, the Media Gateway reset continuously.	100272	1. Insert the modem into port 2 and the flash disk into port 1. 2. Use a US.Robotics 5637 modem instead of the Multitech modem.
G430, G450 One-way talk path occurred when connected to a 3rd party device that changes its source UDP port mid-call. Flash parameter was added to allow field technician to activate or deactivate source UDP port checks.	100524.01	Go back to the previous firmware version.
G430, G450 When one end of a voice call was behind a firewall, the **`traceroute`** packets that the gateway sent to monitor the voice quality of this call, were discarded and no response was received. These **`traceroute`** sessions remained active for a long time, which caused high memory and CPU utilization.	100584	
G430 SNMP set request on **MIB chStatus** caused Communication Manager alarms to be generated.	100743	
All Gateways. The Media Gateways will now use the immediate server originated link recovery after multiple Communication Manager interchanges, instead of the normal link recovery mechanism (keep alive failures) which caused slow registrations.	100780.00	
G430, G450 This fix allows fine tuning by field technicians of the **dtmf detection** function, by way of the **voip parameter 91** (same as TN2602). Previously this voip parameter was not accessible on G430 and G450.	100810	

Table 13: Fixes delivered to Media Gateways 5.2.1 Version 30.15.0 ***2 of 2***

Problem	Keywords	Workaround
G450, G430 An incoming packet sent with broadcast source MAC address (FF:FF:FF:FF:FF:FF) caused connectivity issues. The broadcast address was learnt on the incoming port and any broadcast is now sent to this port instead of being flooded to all ports.	100831.00	

Problems Fixed in Media Gateways 5.2.1 Version 30.14.0

The following fixes were delivered to **Media Gateways 5.2.1 Version 30.14.0.**

Table 14: Fixes delivered to Media Gateways 5.2.1 Version 30.14.0

Problem	Keywords	Workaround
G430, G450 Occasionally the Media Gateway would register with Communication Manager before the VAL board was completely inserted. This caused announcements to not be enabled in Communication Manager, even though they are listed.	100494	
G430 After upgrading the firmware on a G430 from a version older than 30.10.4 to version 30.10.4 or later, you might have experienced clock synchronization issues on the gateway. These issues might have occurred when the G430 is provisioned to synchronize the G430 clocks to an external reference through a DS1 or BRI Media module.	100496	The workaround was to: 1. Turn off the G430. 2. Wait for at least 30 seconds. 3. Turn on the G430.

Known Problems in Media Gateways 5.2.1 Version 30.14.0

This release includes the following known issues in Media Gateways 5.2.1 version 30.14.2.

Table 15: Known problems in Media Gateways 5.2.1 version 30.14.2

Problem	Keywords	Workaround
G450 If you do not configure STP (spanning tree protocol) uniformly, the G450 might not register with the primary Communication Manager Server after a reset.	090595	This behavior is normal. Enable or disable STP on both the G450 LAN port and the peer device connected to G450 LAN port.

Problems Fixed in Media Gateways 5.2.1 Version 30.13.2 (SP3)

The following fixes were delivered to **Media Gateways 5.2.1 version 30.13.2 (SP3).**

Table 16: Fixes delivered to Media Gateways 5.2.1 version 30.13.2 (SP3) ***1 of 2***

Problem	Keywords	Workaround
G430, G450 CCMS traces sent from the gateway to the controller's mst_server had the wrong timestamp.	100387	
G430, G450 The first TTY character of a telephone call using oneX TTY telephone was missing.	100240	
G450 The gateway might have reset because it runs out of file descriptors under maximum voip load with other activity requiring file descriptors. These activities include announcements, telnet sessions, snmp sessions, or web sessions.	100425	

Table 16: Fixes delivered to Media Gateways 5.2.1 version 30.13.2 (SP3) ***2 of 2***

Problem	Keywords	Workaround
G430, G450 Meeting Exchange conference participants heard regular clicking because every 4th to 6th frame represented a10-ms payload instead of the normal 20-ms payload.	100429	
G430, G450 Control messages might have been lost in rare occasions on MP20.	100265	
G430, G450 The Media Gateway did not register to Communication Manager when in the same subnet, because of ARP spoofing prevention The arp entry is now automatically deleted whenever the connection is dropped.	100276	In previous releases you had to disable arp spoofing.
G430, G450 When you set one of the external ports to bind-to-configured vlan-binding-mode, the port was erroneously bound to internal vlan (4093,4094) in addition to the external vlan (1-4090).	100388	
G430, G450 With CM 6.0 and later, the "session icc" CLI command only worked if telnet was enabled on the ICC.	100282	
G430 Gateway DSP capacity dropped from 120 to 100 after a server interchange (PE Dup feature). *G450* Gateway DSP capacity dropped from 320 to 240 after a server interchange (PE Dup feature).	100355	

Known Problems in Media Gateways 5.2.1 Version 30.13.2 (SP3)

This release includes the following known issues in Media Gateways 5.2.1 version 30.13.2 (SP3) (version 30.13.2).

Table 17: Known problems in Media Gateways 5.2.1 version 30.13.2 (SP3)

Problem	Keywords	Workaround
G430 After upgrading the firmware on a G430 Media Gateway from a version older than 30.10.4 to version 30.10.4 and later, you might have clock synchronization issues on the gateway. These issues might occur when the G430 is provisioned to synchronize the G430 clocks to an external reference through a DS1 or BRI Media module.	100496	1. Turn off the G430. 2. Wait for at least 30 seconds. 3. Turn on the G430.
G430 if you connect a Multitech Modem MT5634ZBA-USB to USB port 1 and a USB flash disk to USB port 2, the Media Gateway resets continuously.	100272	1. Insert the modem into port 2 and the flash disk into port 1. 2. Use a US.Robotics 5637 modem instead of the Multitech modem.
G450 If you do not configure STP (spanning tree protocol) uniformly, the G450 might not register with the primary Communication Manager Server after a reset.	090595	This behavior is normal. Enable or disable STP on both the G450 LAN port and the peer device connected to G450 LAN port.

Enhancements in Media Gateways 5.2.1 Version 30.12.1 (SP2)

Disabling the ipsec VPN application

There are two new CLI commands that allow you to disable the ipsec VPN application and view the application's status. This feature is required for certain markets.

disable vpn

Use the **`disable vpn`** command to disable the ipsec VPN feature.

Syntax

`disable vpn`

User level

admin

Context

root

Example

To disable ipsec VPN:

```
Gxx0-001(super)# disable ipsec vpn
```

```
The command will disable the ipsec vpn application on the gateway permanently.
Enable of such application can be done by Avaya Technician only. The command will
reset the gateway. Do you want to continue (Y/N)? Y
```

Important:
Only Services personnel can re-enable ipsec VPN if you disable it.

Note:
If you disable ipsec vpn, then the media gateway resets and starts up without any VPN support. If the startup-config includes VPN commands, then all those commands fail with warning. The running-config is without any VPN commands

show ipsec vpn

Use the show ipsec vpn command to display the ipsec VPN status.

Syntax

show ipsec vpn

User level

admin

Context

root

Example

To show ipsec VPN status:

```
Gxx0-001(super)# show ipsec vpn
IPSEC VPN application is enabled on the gateway
Gxx0-001(super)# show ipsec vpn
IPSEC VPN application is disabled on the gateway
```

Note:

For information on other new features and significant enhancements in Media Gateways 5.2.1, see *Avaya Aura™ Communication Manager Change Description for Release 5.2.1* on http://support.avaya.com.

Problems Fixed in Media Gateways 5.2.1 Version 30.12.1 (SP2)

The following fixes were delivered to **Media Gateways 5.2.1 version 30.12.1 (SP2).**

Table 18: Fixes delivered to Media Gateways 5.2.1 version 30.12.1 (SP2) ***1 of 2***

Problem	Keywords	Workaround
G430 The gateway might not have recognized a USB flash disk inserted in port 2 after a gateway reset. USB port 1 did not have this issue.	100029	Extract then re-insert the USB flash disk in USB port 2 after a reset
G430, G450 Fax/modem detection & in-band DTMF outpulsing were incorrectly disabled when DTMF transport was set to “in-band”. This problem only existed in version 30.11.3.	100287	
G450, G430 On rare occasions, the MP20 lost control messages especially when there was a network traffic burst. This loss might have led to dropped calls.	100203	
G430, G450 The Syslog messages from the gateway did not include the HEADER, which contains the Timestamp and the Hostname.	100206	
G430, G450 The Media Gateway did not offer the option to disable VPN which was turned on by default. See Problems Fixed in Media Gateways 5.2.1 Version 30.12.1 (SP2) on page 30.	100253	
G430 The Media Gateway experienced an exception if it was reset during a boot-up sequence.	100059 100060	
G430, G450 The Media Gateway did not re-register automatically with the controller after the loss of an H.248 link. This was a rare condition caused by the gateway not receiving a response from the controller during the registration process.	100074	

Table 18: Fixes delivered to Media Gateways 5.2.1 version 30.12.1 (SP2) ***2 of 2***

Problem	Keywords	Workaround
G430 When trying to reset the S8300 using the **`reset mm v1`** CLI command, the prompt never returned and the gateway became unstable	100087	
G450, G430 On very rare occasions, voip calls dropped because of voip resources stuck in pending disconnect state. Introduced an audit to cleanup those resources and avoid the dropped calls.	100157	
G430 The Compact Flash LED did not blink when you use the **`test LED`** CLI command.	090449	
G450 If you removed the fan tray then inserts a tray with a non-functioning fan, traps and syslog entries are generated only for the working fans, but not the faulty fan.	090607	Verify visually that all fans work when you replace the fan tray.
G430, G450 The "No dest file for download operation - no download operation was done" message appeared after a media module download, even if the download succeeded.	100054	Verify the download using the **`show module`** CLI command.
G430, G450 When you performed a restore operation from a USB flash disk that includes a media module image, the media module firmware was not updated.	100054	Update the media module firmware manually.
G430, G450 Media Module image names on a USB disk on key that you insert in the Media Gateway were shown in uppercase letters only, regardless of the actual names. This meant that the Media Module image download from the USB disk on key failed The restore procedure also failed.	100056	• Download Media Module firmware using FTP/TFTP. • Perform the restore operation without adding Media Module images to the restore directory.

Problems Fixed in Media Gateways 5.2.1 Version 30.11.3 (SP1)

The following fixes were delivered to **Media Gateways 5.2.1 version 30.11.3 (SP1).**

Table 19: Fixes delivered to Media Gateways 5.2.1 version 30.11.3 (SP1) ***1 of 2***

Problem	Keywords	Workaround
G430, G450 On rare occasions, dialing through a USB modem stops working.	090291	
G430, G450 This release of the media gateway works with versions of Communication Manager earlier than 5.2.1. If you upgrade an LSP to Release 5.2 Service Pack 2 or later, upgrade the corresponding Primary Server to Release 5.2 Service Pack 2 or later, as follows: 1. Upgrade LSP to Release 5.2 Service Pack 2 or later 2. Upgrade Primary Server to Release 5.2 Service Pack 2 or later If you upgrade the LSP to release 5.2 service pack 2 or later, but fail to upgrade the primary server to this release or later, existing and new IP calls might periodically be torn down if the media gateway fails over to the LSP and later falls back to the primary server.	090750	
G430, G450 When you tried to download the authentication file, the following superfluous message appeared: "the banner login command will be disabled after …"	090659	
G430, G450 You could not upload authentication file using a USB flash disk tftp, ftp or scp.	090833	
G430, G450 Third-party equipment that relied on the VoIP Marker bit in DTMF relay did not function correctly because the marker bit was not set.	090669	

Table 19: Fixes delivered to Media Gateways 5.2.1 version 30.11.3 (SP1) ***2 of 2***

Problem	Keywords	Workaround
G430, G450 The destination did not recognize low-amplitude TTY tones that transmitted over VoIP channels because of jitter buffer adjustments	090670	
G430, G450 A traffic burst could have caused the Ethernet receiver to halt and adversely affect VoIP DSP performance. Continuous checking of the Ethernet receiver assures consistent functioning.	090759	
G430, G450 On rare occasions, high traffic with out-of-order packets could have caused the VoIP DSP to reset.	090318	
G430, G450 Running the **`show mm`** CLI command might have displayed all media modules as "Not Installed" although the modules are functional. This display-only issue only occurred after the media modules have reset more than 30 times.	090901	
G430, G450 Incoming VoIP DTMF digits were not detected when they are badly formed. The new firmware greatly improves DTMF digit detection when there is a leading-edge disruption of the digit.	090716	
G430, G450 Sometimes when you did not fully insert a media module, the media module might have been reported as "Unsupported Media Module", even after you fully inserted the media module.	090874	
G430, G450 Fast server interchange in a duplicated main server configuration (PE Dup feature) did not work properly when: • You enabled ARP spoofing, and • Communication Manager and the Media Gateway are on the same subnetwork.	090619	

Problems Fixed in Media Gateways 5.2.1 Version 30.10.4

The following fixes were delivered to **Media Gateways 5.2.1 version 30.10.4.**ë

Table 20: Fixes delivered to Media Gateways 5.2.1 version 30.10.4

Problem	Keywords	Workaround
G430, G450 Outgoing MFC trunk calls failed with "No answer timeout" if using a rule table other than table 0.	090695	
G430 Soft and Hard reset performed by the firmware on the ICC did not work; only a manual reset restored the ICC.	090681	
G430, G450 The list of announcements produced by CLI showed announcements stored in the Compact Flash (CF) even after you removed the CF. The location of the announcements now shows RAM when you remove the CF.	090267	
G430, G450 Passwords with only lowercase letters were accepted.	090560	
G430, G450 On rare occasions, the media gateway might reset during heavy traffic that requires routing between a LAN and a WAN port.	090459	
G430, G450 The CLI stops responding if you run a "copy running-config startup-config" command and end the CLI session before command finishes running (for example, by closing the window). Running any subsequent command generates the "Processing another command please wait…" message.	090410	
G430, G450 VPN ports 500, 2070 and 4500 are open even when VPN is not active.	090443	
G450 Improved performance on the G450 with 320 channels.	090395	

Technical Support

Support for Communication Manager is available through Avaya Technical Support.

If you encounter trouble with Communication Manager:

1. Retry the action. Carefully follow the instructions in written or online documentation.
2. Check the documentation that came with your hardware for maintenance or hardware-related problems.
3. Note the sequence of events that led to the problem and the exact messages displayed. Have the Avaya documentation available.
4. If you continue to have a problem, contact Avaya Technical Support by:
   - Logging in to the Avaya Technical Support Web site http://www.avaya.com/support
   - Calling or faxing Avaya Technical Support at one of the telephone numbers in the Support Directory listings on the Avaya support Web site.

   You may be asked to email one or more files to Technical Support for analysis of your application and its environment.

Note:
If you have difficulty reaching Avaya Technical Support through the above URL or email address, please go to http://www.avaya.com for further information.

When you request technical support, provide the following information:

- Configuration settings, including Communication Manager configuration and browser settings.
- Usage scenario, including all steps required to reproduce the issue.
- Screen shots, if the issue occurs in the Administration Application, one-X Portal, or one-X Portal Extensions.
- Copies of all logs related to the issue.
- All other information that you gathered when you attempted to resolve the issue.

Tip:
Avaya Global Services Escalation Management provides the means to escalate urgent service issues. For more information, see the Escalation Contacts listings on the Avaya Web site.

For information about patches and product updates, see the Avaya Technical Support Web site http://www.avaya.com/support.