Avaya Media Gateways 5.2.1
Version 30.15.0
Release Notes

Issue 1
October 4 2010

Contents

Copyright 2010, Avaya Inc.
All Rights Reserved

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Warranty

Avaya Inc. provides a limited warranty on this product. 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 through the following Web site: http://www.avaya.com/support.

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 may 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 Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at
1-800-643-2353.

Disclaimer

Avaya is not 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. Customer and/or End User agree 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 the Customer or End User.

How to Get Help

For additional support telephone numbers, go to the Avaya support Web site: http://www.avaya.com/support. If you are:

- Within the United States, click the *Escalation Contacts* link that is located under the *Support Tools* heading. Then click the appropriate link for the type of support that you need.
- Outside the United States, click the *Escalation Contacts* link that is located under the *Support Tools* heading. Then click the *International Services* link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

- IEC 60950-1 latest edition, including all relevant national deviations as listed in the IECEE Bulletin—Product Category OFF: IT and Office Equipment.
- CAN/CSA-C22.2 No. 60950-1 / UL 60950-1 latest edition.

This product may contain Class 1 laser devices.

- Class 1 Laser Product
- Luokan 1 Laserlaite
- Klass 1 Laser Apparat

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards, as applicable:

- CISPR 22, including all national standards based on CISPR 22.
- CISPR 24, including all national standards based on CISPR 24.
- IEC 61000-3-2 and IEC 61000-3-3.

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.

Federal Communications Commission Part 15 Statement:

For a Class A digital device or peripheral:

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

For a Class B digital device or peripheral:

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Equipment With Direct Inward Dialing ("DID"):

Allowing this equipment to be operated in such a manner as to not provide proper answer supervision is a violation of Part 68 of the FCC's rules.

Proper Answer Supervision is when:

A. This equipment returns answer supervision to the public switched telephone network (PSTN) when DID calls are:

- answered by the called station,
- answered by the attendant,
- routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user
- Routed to a dial prompt

B. This equipment returns answer supervision signals on all (DID) calls forwarded back to the PSTN.

Permissible exceptions are:

- A call is unanswered
- A busy tone is received
- A reorder tone is received

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

Automatic Dialers:

When programming emergency numbers and (or) making test calls to emergency numbers:

- Remain on the line and briefly explain to the dispatcher the reason for the call.
- Perform such activities in the off-peak hours, such as early morning or late evenings.

Toll Restriction and least Cost Routing Equipment:

The software contained in this equipment to allow user access to the network must be upgraded to recognize newly established network area codes and exchange codes as they are placed into service.

Failure to upgrade the premises systems or peripheral equipment to recognize the new codes as they are established will restrict the customer and the customer's employees from gaining access to the network and to these codes.

For equipment approved prior to July 23, 2001:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover of this equipment is a label that contains, among other information, the FCC registration number, and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

For equipment approved after July 23, 2001:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council on Terminal Attachments (ACTA). On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXX. If requested, this number must be provided to the telephone company.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0.
L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas cinq.
To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXX. The digits represented by ## are the REN without a decimal point (for example, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Means of Connection:

Connection of this equipment to the telephone network is shown in the following table:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2.T	AS.2	RJ2GX, RJ21X, RJ11C
CO trunk	02GS2	0.3A	RJ21X, RJ11C
	02LS2	0.3A	RJ21X, RJ11C
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9.BN	6.0F	RJ48C, RJ48M
	04DU9.1KN	6.0F	RJ48C, RJ48M
	04DU9.1SN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9.DN	6.0Y	RJ48C

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at

1-800-242- 2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Installation and Repairs

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. It is recommended that repairs be performed by Avaya certified technicians.

FCC Part 68 Supplier's Declarations of Conformity

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

Canadian Conformity Information

This Class A (or B) digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A (ou B) est conforme à la norme NMB-003 du Canada.

This product meets the applicable Industry Canada technical specifications/Le présent materiel est conforme aux specifications

techniques applicables d'Industrie Canada.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (Conformité Europeénne) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (2004/108/EC) and Low Voltage Directive (2006/95/EC).

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

European Union Battery Directive

Avaya Inc. supports European Union Battery Directive 2006/66/EC. Certain Avaya Inc. products contain lithium batteries. These batteries are not customer or field replaceable parts. Do not disassemble. Batteries may pose a hazard if mishandled.

Japan

The power cord set included in the shipment or associated with the product is meant to be used with the said product only. Do not use the cord set for any other purpose. Any non-recommended usage could lead to hazardous incidents like fire disaster, electric shock, and faulty operation.

本製品に同梱または付属している電源コードセットは、本製品専用です。本製品以外の製品ならびに他の用途で使用しないでください。火災、感電、故障の原因となります。

If this is a Class A device:

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラス Ａ 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

If this is a Class B device:

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラス Ｂ 情報技術装置です。この装置は，家庭環境で使用することを目的としていますが，この装置がラジオやテレビジョン受信機に近接して使用されると，受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site:

http://www.avaya.com/support

Changes Delivered to Media Gateways 5.2.1 Version 30.15.0

Media Gateways 5.2.1 Version 30.15.0 Release Notes

Media Gateway firmware releases and versions are cumulative. Media Gateways 5.2.1 Version 30.15.0 includes the following Media Gateway firmware versions:

- 30.14.0
- 30.13.2
- 30.12.1
- 30.10.4
- 29.24.4
- 29.24.3
- 29.24.2
- 29.24.1
- 29.24.0
- 29.23.0
- 29.22.3

The changes delivered to Media 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.

Enhancements

For information on 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 30.15.0

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

Table 1: 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 intoport 1. 2. Use a US.Robotics 5637 modem instead of the Multitech modem.
G430, G450, IG550 One-way talk path occured 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, IG550 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	
IG550. Only **ICMP Echo-Request** packets sent to a broadcast address should be ignored, but all **ICMP Echo-Requests** were being ignored.	100806	

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

Problem	Keywords	Workaround
G430, G450,IG550. 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	
G450, G430, IG550. 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	

Known Problems in Media Gateways 5.2.1 Version 30.15.0

This release includes the following known issues in Media Gateways 5.2.1 Version 30.15.0.

Table 2: Known problems in Media Gateways 5.2.1 Version 30.15.0

Problem	Keywords	Workaround
G450 When STP was not configured (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.

Changes Delivered to Previous Media Gateways 5.2.1 Versions

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 3: Fixes delivered to Media Gateways 5.2.1 Version 30.14.0

Problem	Keywords	Workaround
G250, G350, G430, G450, G700, IG550 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 4: 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 5: Fixes delivered to Media Gateways 5.2.1 version 30.13.2 (SP3) ***1 of 3***

Problem	Keywords	Workaround
G700 In rare occasions, the gateway encountered an exception possibly leading to a H,248 link bounce.	100389	
G250, G350, G430, G450, G700, IG550 CCMS traces sent from the gateway to the controller's mst_server had the wrong timestamp.	100387	
G430, G450, IG550 The first TTY character of a telephone call using oneX TTY telephone was missing.	100240	

Table 5: Fixes delivered to Media Gateways 5.2.1 version 30.13.2 (SP3) ***2 of 3***

Problem	Keywords	Workaround
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	
G430, G450, IG550 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, IG550 Control messages might have been lost in rare occasions on MP20.	100265	
G250, G350, G430, G450, G700, IG550 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.
G700 All static routes, including the default gateway, might have been lost after deleting one static route then resetting the gateway.	100300	
G700 On rare occasions, the gateway rebooted because of an exception in the tCli task after logging into the gateway CLI.	100373	
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	
G250, G350, G430, G450 With CM 6.0 and later, the "session icc" CLI command only worked if telnet was enabled on the ICC.	100282	

Table 5: Fixes delivered to Media Gateways 5.2.1 version 30.13.2 (SP3) ***3 of 3***

Problem	Keywords	Workaround
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 6: Known problems in Media Gateways 5.2.1 version 30.13.2 (SP3) ***1 of 2***

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.

Table 6: Known problems in Media Gateways 5.2.1 version 30.13.2 (SP3) ***2 of 2***

Problem	Keywords	Workaround
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 7: Fixes delivered to Media Gateways 5.2.1 version 30.12.1 (SP2) ***1 of 3***

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
G700 The **`show ip route`** CLI command output displayed an internal IP address starting with 169.254.1	100192	
G430, G450, IG550 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, IG550 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	
G250, G350, G450, G430 The Syslog messages from the gateway did not include the HEADER, which contains the Timestamp and the Hostname.	100206	
G250, G350, 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 21.	100253	
G430 The Media Gateway experienced an exception if it was reset during a boot-up sequence.	100059 100060	

Table 7: Fixes delivered to Media Gateways 5.2.1 version 30.12.1 (SP2) *2 of 3*

Problem	Keywords	Workaround
G250-DS1, IG550 Enabling echo cancellation interfered with clear channel or data connections over DS1 trunks.	100068	
G250, G350, G430, G450, *IG550* 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	
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, *IG550* 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.
G250, G350, G450, G430 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.
G350, G450, G430 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.

Table 7: Fixes delivered to Media Gateways 5.2.1 version 30.12.1 (SP2) ***3 of 3***

Problem	Keywords	Workaround
G350, 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 8: Fixes delivered to Media Gateways 5.2.1 version 30.11.3 (SP1) ***1 of 3***

Problem	Keywords	Workaround
G250, G350, G450, G430 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	
G250, G350, G450, G430, IG550 When you tried to download the authentication file, the following superfluous message appeared: "the banner login command will be disabled after ..."	090659	
G250, G350, G450, G430, IG550 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 8: Fixes delivered to Media Gateways 5.2.1 version 30.11.3 (SP1) ***2 of 3***

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	
G350 Mibwalk failed because of the survivability MIB on G350 hardware C/S:1 (vintage 1.A) that did not support survivability. Use the **`show system`** CLI command to check the hardware vintage.	090475	
G250, G350, G430, G450, IG550 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	
G250, G350, 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	

Table 8: Fixes delivered to Media Gateways 5.2.1 version 30.11.3 (SP1) ***3 of 3***

Problem	Keywords	Workaround
G250, G350, G430, G450, IG550, G700 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.**

Table 9: Fixes delivered to Media Gateways 5.2.1 version 30.10.4

Problem	Keywords	Workaround
G250, G350, G430, G450, IG550, G700 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	
G250, G350, G430, G450, IG550, G700 Passwords with only lowercase letters were accepted.	090560	
G250, G350, G430, G450 On rare occasions, the media gateway might reset during heavy traffic that requires routing between a LAN and a WAN port.	090459	
G250, G350, G430, G450, IG550 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	
G250, G350, G430, G450, IG550 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.