WB.15.12.0015 Software Fix List

Contents

Description

This fix list covers software versions beginning with WB.15.12.0006.

Version WB.15.12.0006 was the initial release of Major version WB.15.12 software. WB.15.12.0006 software was built from the same source as WB.15.11.0003. WB.15.12.0006 includes all enhancements and fixes in WB.15.11.0003 software, plus the additional enhancements and fixes in the WB.15.12.0006 fix list (below).

Here is a visual depiction of the software sequence, showing how each Major version (for example WB.15.12) is based on the previous Major version - and then additional fixes are added to Minor versions (for example WB.15.12.0007). This depiction shows the two most recent Major versions and all the Minor versions that have been built at the time of this publication.

```
WB.15.11.0003 --> WB.15.11.0004 --> WB.15.11.0005 --> WB.15.11.0006 --> WB.15.11.0007 -->
          |       WB.15.11.0008 --> WB.15.11.0009
          v
WB.15.12.0006 --> WB.15.12.0007 --> WB.15.12.0008 --> WB.15.12.0010 --> WB.15.12.0011 -->
                  WB.15.12.0012 --> WB.15.12.0013 --> WB.15.12.0014 --> WB.15.12.0015
                  (WB.15.12.0009 was never built)
```

Note: WB.15.11.0003 was the first software version for the HP 2920 switches.

These documents are included in the WB.15.12.0015 software zip file:

- Release Notes Basic Information Guide
- WB.15.12.0015 Fix List

Product Models

HP 2920-24G Switch	(J9726A)
HP 2920-48G Switch	(J9728A)
HP 2920-24G-PoE+ Switch	(J9727A)
HP 2920-48G-PoE+ Switch	(J9729A)
HP 2920-48G-PoE+ 740W Switch	(J9836A)

Enhancements

Version WB.15.12.0006 Enhancements

Enhancement (PR_0000072866, CR_0000077692) - RADIUS IPv6. This enhancement adds IPv6 capabilities for the RADIUS client. The Network Access Server will be able to use IPv6 addresses as well as communicating with IPv6 RADIUS servers. See "RADIUS Authentication, Authorization, and Accounting" in the *Access Security Guide*. See also the *IPv6 Configuration Guide* for your switch.

Enhancement (CR_0000106140) - Flight Data Recorder Phase 2. The Flight Data Recorder provides a way to capture and preserve data that is related to a crash event. Phase 2 adds the capture and preservation of protocol and subsystem-specific information.

Enhancement (CR_0000107011) - CDPv2 Transmit Capability. When a Cisco VoIP phone boots up (or sometimes periodically), it queries the switch and advertises information about itself using CDPv2. The switch receives the VoIP VLAN Query TLV (type 0x0f) from the phone and then immediately sends the voice VLAN ID in a reply packet to the phone using the VLAN Reply TLV (type 0x0e). The phone then begins tagging all packets with the advertised voice VLAN ID.

Enhancement (CR_0000109154) - OpenFlow. OpenFlow is a programmable open-standard network protocol that uses flexible matching rules to classify and manage network traffic into flows. For more information, see the *OpenFlow Configuration Guide*.

Enhancement (CR_0000113486) - Readable Interface Names in Traps. The SNMP trap notification messages for linkup and linkdown events on an interface now include IfDesc and IfAlias var-bind information. For more information on SNMP traps, see "Configuring for Network Management Applications" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000119734) - Event Log Severity Changes. The default severity status of several event log messages has been changed from "informational" to "warning". See the *Event Log Message Reference Guide* for more information about event log messages.

Enhancement (CR_0000122671) - Strict Priority Queueing. The switches currently implement priority-to-queue mapping as defined in the IEEE 802.1D-2004 Annex G standard. Another standard, IEEE 802.1Q-2005, defines a slightly different mapping where the ordering of priorities 0-2 is changed. This enhancement allows you to configure the switch to follow either standard.

Enhancement (CR_0000123824) - Clarify Port VLAN Tagged Status. This enhancement allows the identification of ports as "access", "trunk", or "voice". The **show interfaces** command has added the **status** option which displays tagged and untagged VLAN information for a port. See "Static Virtual LANs (VLANs)" in the *Advanced Traffic Management Guide* for your switch.

Prerequisites

Minimum Software Versions

Product Number	Product Name	Minimum Supported Software Version
J9805A	HP 640 Redundant/External Power Supply Shelf	WB.15.13.0003

Fixes

Software fixes are listed in chronological order, from oldest to newest software version. Unless otherwise noted, each software version listed below includes all the software fixes and enhancements added in previous versions listed below.

WB.15.11.0003 was the first software version for the HP 2920 switches.

Version WB.15.12.0006 Fix List

Status: Released and fully supported, and posted on the web.

Enhancement (PR_0000072866, CR_0000077692) - RADIUS IPv6. This enhancement adds IPv6 capabilities for the RADIUS client. The Network Access Server will be able to use IPv6 addresses as well as communicating with IPv6 RADIUS servers. See "RADIUS Authentication, Authorization, and Accounting" in the *Access Security Guide*. See also the *IPv6 Configuration Guide* for your switch.

Enhancement (CR_0000106140) - Flight Data Recorder Phase 2. The Flight Data Recorder provides a way to capture and preserve data that is related to a crash event. Phase 2 adds the capture and preservation of protocol and subsystem-specific information.

Enhancement (CR_0000107011) - CDPv2 Transmit Capability. When a Cisco VoIP phone boots up (or sometimes periodically), it queries the switch and advertises information about itself using CDPv2. The switch receives the VoIP VLAN Query TLV (type 0x0f) from the phone and then immediately sends the voice VLAN ID in a reply packet to the phone using the VLAN Reply TLV (type 0x0e). The phone then begins tagging all packets with the advertised voice VLAN ID.

Enhancement (CR_0000109154) - OpenFlow. OpenFlow is a programmable open-standard network protocol that uses flexible matching rules to classify and manage network traffic into flows. For more information, see the *OpenFlow Configuration Guide*.

Enhancement (CR_0000113486) - Readable Interface Names in Traps. The SNMP trap notification messages for linkup and linkdown events on an interface now include IfDesc and IfAlias var-bind information. For more information on SNMP traps, see "Configuring for Network Management Applications" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000119734) - Event Log Severity Changes. The default severity status of several event log messages has been changed from "informational" to "warning". See the *Event Log Message Reference Guide* for more information about event log messages.

Enhancement (CR_0000122671) - Strict Priority Queueing. The switches currently implement priority-to-queue mapping as defined in the IEEE 802.1D-2004 Annex G standard. Another standard, IEEE 802.1Q-2005, defines a slightly different mapping where the ordering of priorities 0-2 is changed. This enhancement allows you to configure the switch to follow either standard.

Enhancement (CR_0000123824) - Clarify Port VLAN Tagged Status. This enhancement allows the identification of ports as "access", "trunk", or "voice". The **show interfaces** command has added the **status** option which displays tagged and untagged VLAN information for a port. See "Static Virtual LANs (VLANs)" in the *Advanced Traffic Management Guide* for your switch.

Loop Protection (CR_0000109506) - In some cases, loop protection fails to disable the port.

SSH (PR_0000072707, CR_0000077550) - The switch allows unlimited SSH connection attempts. With this fix, the switch's SSH server goes into a 60-second timeout period after three consecutive unsuccessful login attempts.

Version WB.15.12.0007 Fix List

Status: Released and fully supported, but not posted on the web.

Crash (CR_0000127335) - In some situations, issuing the **show tech all** command might cause the switch to reboot unexpectedly with a message similar to `Length Corruption`.

Uplink Failure Detection (CR_0000127868) - On a switch that is configured for uplink failure detection where the link to monitor (LtM) or link to disable (LtD) is an LACP trunk, after reboot the link to monitor is listed as `down` in the output of **show uplink-failure-detection**, and the link to disable is taken down by the switch.

Version WB.15.12.0008 Fix List

Status: Released and fully supported, but not posted on the web.

Authentication (CR_0000134114) - With both 802.1X and MAC Authentication configured on a port, it is possible for an already-authenticated client to be erroneously moved to the unauthenticated VLAN.

Banner MOTD (CR_0000132198) - The login banner is not displayed if the user logs into the switch via the standby or member switch instead of the active or commander switch.
Crash (CR_0000126777) - With a combination of interface state changes along with IPV6 address configuration changes, it is possible for the switch to reboot unexpectedly with a message similar to `SubSystem 0 went down:  01/24/13 13:31:29, Invalid Instr HW Addr=0x000004a8 IP=0x4a8, Task='mIpCtrl' Task ID=0xa9ca140 sp:0x470aab0 lr:0x723f4c, msr: 0x02029200 xer: 0x20000000 cr: 0x48000400`.

Crash (CR_0000129047) - When running commands from multiple simultaneous CLI sessions the switch may reboot with the error message `Software exception at hwBp.c:218.`

Dynamic ARP Protection (CR_0000132073) - When a VLAN is configured for dynamic ARP protection and also DHCP snooping, ARP packets should be forwarded but are incorrectly dropped when the **arp-protect** configuration does not include the **validate ip** option.

GVRP (CR_0000129917) - When the switch receives its own GVRP frames, it learns from them instead of dropping the frames.

GVRP (CR_0000130090) - After rebooting the switch, the configuration **unknown-vlans disable** does not work on trunks.

IGMP (CR_0000134412) - The switch sends an IGMP General Query with an incorrect layer 2 destination address.

Loop Protection (CR_0000127150) - Loop protection fails to detect a loop on a port configured for 802.1X authentication, if 802.1X is not enabled globally.

Management (CR_0000134091) - Disabling write access to an SNMP community via the Web user interface might cause the switch to become unresponsive to command input. The switch must be rebooted to regain management access.

Passwords (CR_0000130921) - If the switch is configured with a username and password, changing the password causes the username to also change. The username is changed to the default "manager" or "operator", depending on which password is changed.

Passwords (CR_0000134675) - The switch does not automatically create a default username of "manager" or "operator" when a password is configured for those levels of access.

SNMP (CR_0000122623) - After rebooting a switch configured for SNMP with the parameters **operator unrestricted**, the switch does not allow the user to set any read/write MIB objects.

Stacking (CR_0000121075) - When stacking is enabled, the switch is accessible via the Web even after disabling the Web server, and via TELNET even after disabling TELNET.

Transceivers (CR_0000133023) - 100-Megabit transceivers might have one or more of these symptoms: 1) Link LED is lit but link is down, 2) No Link after the transceiver is hot-swapped, 3) Transceiver fails self test.

Version WB.15.12.0009

Status: Never built.

Version WB.15.12.0010 Fix List

Status: Released and fully supported, and posted on the web.

CLI (CR_0000137287) - The output of **show run vlan <VLAN_ID>** omits the **no** in the configuration entry **no ip igmp fastleave**. Note that the output of **show run** gives correct information.

Config (CR_0000131054) - Setting an operator or manager password on the switch causes four features to be disabled: auto run, DHCP-based config file download from an external tftp server, DHCP-based software image download from an external tftp server, and tftp server functionality within the switch. With this fix, more accurate messages are sent regarding the specific features that are disabled by setting the operator or manager password.

Config (CR_0000135481) - After boot, a config file that has a trap destination community name with an open parenthesis "(" or a close parenthesis ")" cannot be downloaded to the switch.

Crash (CR_0000127791) - With OSPF configured, in a rare situation the switch might reboot unexpectedly with a message similar to `Software exception at rt_table.c:4453 -- in 'eRouteCtrl', task ID = 0xa9c4c00 -> Routing Stack: Assert Failed`. This improves the original Crash fix (CR_0000120116).

Crash (CR_0000130339) - In some situations, executing the command **show snmp-server traps** might cause the switch to reboot unexpectedly with a message similar to `Software exception at cli_snmpv2_action.c:9634 -- in mSess2', task ID = 0x13ab0 -> ASSERT: failed`.

Crash (CR_0000131604) - Configuring Mac Authentication with a 256-client limit might cause the switch or stack member to reboot unexpectedly.

Crash (CR_0000131959) - With MAC Authentication configured on stacking ports, the switch might reboot unexpectedly with a message similar to `Software exception at highAvailHelper.c:1040 -- in 'mRdHelper', task ID = 0x3c9389c0`.

Event Log (CR_0000127436) - After the switch uptime reaches 497 days, the timestamp entries in the event log become erratic with gaps of several hours or days. In some cases the timestamps revert to previous months and years, even though SNTP updates with those wrong timestamps report the correct date and time.

IGMP (CR_0000132149) - Although the RFC requires that the switch with the lowest IP address becomes querier, a switch that is acting as querier stops being querier when it receives a query from a switch with a higher IP address.

IGMP (CR_0000135527) - A non-querier switch that receives a Join from the querier fails to send further Joins to the querier, resulting in loss of multicast traffic.

Latency (CR_0000132667) - After a switch reboot, traffic that flows through the J9538A 8-port 10GbE SFP+ v2 zl Module experiences poor performance.

Link (CR_0000137549) - Gigabit fiber transceivers operate in auto-negotiation mode even if the port is configured for 1000 Mbps full-duplex operation (**speed-duplex 1000-full**). If both sides of the link were configured as 1000-full, the link will go down after the switch at one side of the link is updated with affected software. This issue was introduced in software version 15.12.0006.

MAC Authentication (CR_0000129991) - MAC Authentication fails when the **peap-mschapv2** parameter is included in the **aaa authentication** CLI command.

Menu (CR_0000135171) - With the Menu interface, if the user navigates to Switch Configuration -> IP Configuration and selects Save without changing anything on that screen, OSPF settings are removed from every VLAN.

OpenFlow (CR_0000134471) - OpenFlow flows are not programmed correctly when RPVST+ is disabled on the OpenFlow member VLAN.

Passwords (CR_0000134358) - Navigating to the security wizard page on a switch that has manager and operator credentials set, a tool such as firebug allows the admin to view passwords in the secwiz.js file. (The admin would have to be logged in with valid credentials in order to view the passwords.)

Routing (CR_0000123230) - The switch does not forward traffic to a host that has a static route configured with a 32-bit subnet mask. Traces show that the switch never sends an ARP request for that host.

sFlow (CR_0000128439) - When an sFlow-sampled inbound packet is to be routed, the sFlow data gives the wrong output port on the switch.

Web Management (CR_0000135883) - The "Rx Errors" column is missing from the Web user interface.

Version WB.15.12.0011 Fix List

Status: Released and fully supported, but not posted on the web.

Accounting (CR_0000133762) - If a Windows system is configured for both computer authentication and user authentication, accounting might not function properly.

DHCP (CR_0000137877) - A switch acting as a DHCP relay agent sends two DHCP packets, one of which incorrectly has the source MAC address of the client instead of the switch.

RADIUS Accounting (CR_0000137793) - An interim-update status request generates incorrect accounting information in the RADIUS server.

Web Management (CR_0000137792) - A self-signed SSL certificate generated via the Web interface cannot use a common name (CNAME) longer than 40 characters. With this fix, the limit is 90 characters.

Version WB.15.12.0012 Fix List

Status: Released and fully supported, but not posted on the web.

Config (CR_0000138447) - After a switch software update, SNMP community access privileges are incorrectly changed by the switch. The output of **show snmp-server** and the output of a "walkmib" command give different results, and neither output represents how the switch actually behaves for Manager or Operator access. This issue was introduced with CR_0000122623; if the access settings were configured on a switch without the CR_0000122623 fix, after updating to software with the CR_0000122623 fix the settings are changed.

Crash (CR_0000135900) - In some situations it is possible for the switch to reboot unexpectedly with a message similar to `Software exception at alloc_free.c:646 -- in 'eDrvPoll', task ID = 0xa9a7a80 -> buf already freed by 0x0A9A7D40, op=0x0006003E`.

Crash (CR_0000137288) - With SNTP configured, in a rare situation after a time update the switch might reboot unexpectedly with a message similar to `Health Monitor: Invalid Instr Misaligned Mem Access HW Addr=0x31352e30 IP=0x31352e30 Task='mDebugCtrl' Task ID=0x3c9558c0 sp:0x11f92cd0 lr:0x31352e31 msr: 0x02029200 xer: 0x00000000 cr: 0x28000800`.

Crash (CR_0000138879) - After boot, a switch that has a syslog server and an IPv6 address configured might become unresponsive to management, and after a period of time the switch might reboot repeatedly with a message similar to `NMI event SW:IP=0x001517d4 MSR:0x02029200 LR:0x0015178c cr: 0x28000400 sp:0x03aae0e0 xer:0x00000000 Task='mDebugCtrl' Task ID=0xa9f8000`.

Guaranteed Minimum Bandwidth (CR_0000136039) - When the switch is configured to use fewer than the default of 8 queues, packets in lower-priority queues might be unintentionally dropped.

ICMP (CR_0000134682) - The switch does not log an unsolicited ICMP reply unless it has first pinged some (any) IP address. Also, unsolicited ICMP reply log messages are sometimes associated with the DEFAULT_VLAN instead of the VLAN of the incoming unsolicited ICMP reply.

Jumbo Frames (CR_0000137961) - When jumbo frames are enabled on any VLAN, OSPF fails to establish an adjacency after a switch reboot, and RIP updates might not be accepted by the router.

Policy Based Routing (CR_0000134936) - The **show statistics policy** counter is not reset by the **clear statistics policy** command.

sFlow (CR_0000134427) - sFlow sampling of multicast packets sometimes results in duplicate packets that can cause pixelation of video or other degradation of the multicast stream.

TFTP (CR_0000132721) - Certain lines in the configuration file are sometimes incorrectly changed when imported via TFTP. For example, the configuration entry **snmp-server community public unrestricted** might have the **unrestricted** parameter removed when the config file is downloaded via TFTP.

Web Management (CR_0000139666) - Customers using a browser that does not support the X-Frame-Options tag, and who have an open Web management session and then initiate another browser session, could be vulnerable to cross-frame scripting.

Web Management (CR_0000140379) - A self-signed SSL certificate and a CA-generated certificate cannot use an organizationName, organizationalUnitName, localityName, stateOrProvinceName longer than 40 characters. With this fix, the limit is 64 characters.

Version WB.15.12.0013 Fix List

Status: Released and fully supported, but not posted on the web.

Config (CR_0000142393) - Upgrading software from WB.15.11.xxxx to a newer version changes the **console inactivity-timer** from the configured value in minutes to that same value in seconds. Also, if the **console idle-timeout** value is set, after reboot the configured value is used for a console connection but not a TELNET connection.

Fastboot (CR_0000141043) - If the fastboot setting is changed by the user, and the switch experiences a power interruption or reboot while the new setting is being written to flash, upon bootup the MAC address on a stack member might be erased. Note that this fix has a side effect: If the fastboot setting is changed by the user and the switch software is downgraded (changed to an earlier version), upon bootup the fastboot setting might revert to what it was before the user-initiated change, even though the switch reports that it has been changed. Workaround: Change the fastboot setting twice - first change it back to what it was before the user-initiated change, then change fastboot to the desired setting.

Version WB.15.12.0014 Fix List

Status: Released and fully supported, and posted on the web.

BGP (CR_0000138230) - When BGP has equal cost routes but one route is preferred due to a higher configured weight, the outputs of **show ip bgp** and **show ip route** show that the router uses the wrong route.

Counters (CR_0000142198) - When a trunk configured for sFlow polling is simultaneously queried via SNMP, all counter values for the trunk are zero.

Crash (CR_0000141095) - When a switch port is configured for MAC authentication with the **addr-moves** parameter, if a client on that port moves to a different port the switch might reboot unexpectedly with a message similar to `Software exception at hwBp.c:218 -- in 'fault_handler', task ID = 0xa5df1c0 -> MemWatch Trigger: Offending task 'mWebAuth'. Offending IP=0xb35494`.

Crash (CR_0000142134) - With outbound queue monitoring configured (**qos watch-queue <PORT>**), a switch module or port bank might reboot unexpectedly with a message similar to `Software exception at alloc_free.c:793 -- in 'mAsicUpd', task ID = 0x61e7b00 -> buf already freed by 0x061E7B00, op=0x00500079`.

Crash (CR_0000143459) - When a switch is added to a physical stack, if either the new switch or the stack (but not both) is running a version of software listed below, the stack might reboot unexpectedly with a message similar to `Software exception at proStackUtil.c:137 -- in 'mStackingCtrl', task ID = 0x3c940dc0`. The applicable software versions are KA.15.12.0012 (for 3800 switches), and WB.15.12.0012 and WB.15.12.0013 (for 2920 switches).

Display Issue (CR_0000140830) - When **terminal length** is changed from the default of 24, the config file display is truncated, and the outputs of **show logging** and **show interfaces** might be interleaved in the output of **show tech all**.

Meshing (CR_0000143068) - Multicast traffic and unicast traffic with unknown destination addresses are not routed over the mesh.

RADIUS (CR_0000138258) - In some situations, the switch response to Change of Authorization and Disconnect Messages from the RADIUS server is sent from an incorrect source IP address, which the RADIUS server therefore ignores.

Spanning Tree (CR_0000143817) - With a switch configured for MSTP, if the spanning tree mode is changed to **force-version rstp-operation** and then a second management module (or stack member) is inserted, the switch might reboot unexpectedly with a message similar to `Health Monitor: Read Error Restr Mem Access HW Addr=0xe59ff10c IP=0x779004c Task='mMstpCtrl' Task ID=0x13af9740 fp: 0x0d372620 sp:0x0d372604 cpsr: 0x6000001f`.

Version WB.15.12.0015 Fix List

Status: Released and fully supported, and posted on the web.

Config (CR_0000145562) - A switch with an active radio port and configured with the command **lldp auto-provision radio-ports auto-vlan 2100** will move the radio ports into VLAN 2101 after a reboot. Similar errors occur for other **auto-vlan** numbers; after reboot the switch creates and uses a new VLAN instead of using the configured VLAN for radio ports.

Console (CR_0000140941) - The **console inactivity-timer** setting is applied even if the user is typing on the console, when the console physical connection is to a stack member instead of the commander.

Counters (CR_0000141119) - The output of **show ip counters** is incorrect when routing is enabled for IP, IPv6, or multicasts.

Counters (CR_0000143860) - On a switch configured with rapid PVST and BPDU protection, the output of the command **show spanning-tree bpdu-protection** shows zero `errant BPDUs` received, even when the switch has disabled a port due to receiving a BPDU. This is a display issue only, both rapid PVST and BPDU protection function properly.

Crash (CR_0000133659) - With sFlow enabled and IPv6 configured on a VLAN, the switch might reboot unexpectedly with a message similar to `Software exception at sflow.c:5563 -- in 'mEaseCtrl', task ID = 0x3c8c1680`.

Crash (CR_0000142238) - From the menu, after selecting "Status and Counters" and "Port Address Table" for an active port, the switch might reboot unexpectedly with a message similar to `Read Error Restr Mem Access HW Addr=0x2020201c IP=0x4ee7ce8 Task='mSess1' Task ID=0xe087cc0 fp: 0x06cefc48 sp:0x06cefc20 cpsr: 0x2000001f dfsr: 0x00000005`.

Crash (CR_0000144879) - The switch might reboot unexpectedly in these situations:
1) The switch is running 15.08 or earlier software, is configured to drop frames that have a destination address of 01:00:0c:cc:cc:cd, and has PVST filtering or PVST protection enabled. Then the switch is updated to 15.09 or later software.
2) The switch is running 15.09 or later software, is configured to drop frames that have a destination address of 01:00:0c:cc:cc:cd, and then PVST filtering or PVST protection is enabled.
The switch reboots unexpectedly with a message similar to `Software exception at bttfLearn.c:2616 -- in 'mLpmgrCtrl', task ID = 0xa98a9c0 -> Mac Table Error`.

Crash (CR_0000146306) - The switch uses TCP connections internally for inter-process communication. In a situation where an internal loopback TCP socket pair receives stimulus after an extended period of idle time, the switch might reboot unexpectedly with a message similar to `NMI event SW:IP=0x00e20c1c MSR:0x02029200 LR:0x00e077d0 cr: 0x44000400 sp:0x02b03c58 xer:0x00000000 Task='InetServer' Task ID=0xab31000`.

IGMP (CR_0000138408) - Joins sent by clients in response to a Group Specific Query are not forwarded by the Querier, causing the clients to lose the stream.

IGMP (CR_0000140514) - After disabling IGMP forwarding on a port, multicast traffic incorrectly continues to flow from that port.

Mirroring (CR_0000145818) - With more than one remote mirroring session configured on a VLAN, if the user deletes a VLAN with a lower number than the VLAN being mirrored, all mirrors except the lowest-numbered mirror session are removed from the mirrored VLAN.

Multicast (CR_0000138817) - When a multicast stream is sent to a reserved multicast address, a General Query might not be not forwarded by the switch, causing clients to be dropped from the multicast stream.

Switch Hang (CR_0000146247) - With both authentication and accounting enabled, the switch might become unresponsive to management, requiring a reboot to recover.

TELNET (CR_0000127908) - Continuous logging on and then logging off via TELNET might cause the switch to believe all TELNET sessions are in use, and no additional TELNET sessions can be established.

March 2014

Return to Contents