avaya.com

Virtual Services Platform 9000
Software Release 3.3.4

1. Release Summary

Release Date: June 2013
Purpose: Software release to address customer found software issues.

2. Important Notes before Upgrading to This Release

None.

3. Platforms Supported

Virtual Services Platform 9000 (all models)
.

4. Special Instructions for Upgrade from previous releases

None.

5. Notes for Upgrade

Please see "*Virtual Services Platform 9000, Release Notes*" for software release 3.3.0.0 (NN46250-401, 04.02) available at http://www.avaya.com/support for details on how to upgrade your Switch.

File Names For This Release

File Name	Module or File Type	File Size (bytes)
VSP9K.3.3.4.0.tgz	Release 3.3.4.0 archived software distribution	105019615
VSP9K.3.3.4.0_modules.tgz	Release 3.3.4.0 Encryption Modules	39423

Note about image download:

Ensure images are downloaded using the binary file transfer.

Check that the file type suffix is ".tgz" and the image names after download to device match those shown in the above table. Some download utilities have been observed to append ".tar" to the file name or change the filename extension from ".tgz" to ".tar". If file type suffix is ".tar" or file name does not exactly match the names shown in above table, rename the downloaded file to the name shown in the table above so that the activation procedures will operate properly.

©2013 Avaya Inc. Revision 01.02

Load activation procedure:

software add VSP9K.3.3.4.0.tgz
software add-modules 3.3.4.0.GA VSP9K.3.3.4.0_modules.tgz
software activate 3.3.4.0.GA

6. Version of Previous Release

Software Version 3.3.2,3.3.2.1, and 3.3.3

7. Compatibility

Although this release does not support the Multicast over SPBm feature, Release 3.3.2 is the minimum required release to interoperate with an ERS 8800 7.2 switch with Multicast over SPBm. In addition, Release 3.3.2 or greater is recommended to fully interoperate with ERS 8800 7.2 SPBm network deployment.

8. Changes in 3.3.4

New Features in This Release

No new features in this release

Old Features Removed From This Release

No features removed from this release.

Problems Resolved in This Release

ID	Description
wi01080455	SF1 may core when chassis is booting up from cold boot and all cards are populated.
wi01082799	Add support for new CWDM SPF+ pluggables 10G ER CWDM 1470nm - 1610nm AA1403153-E6 - AA1403160-E6 10G ZR CWDM 1470nm - 1610nm AA1403161-E6 - AA1403168-E6
wi01094483	Some spelling errors in rapid_city_vsp mib
wi01094071	VSP doesn't respond to SNMP queries if NTP is disabled.
wi01085453	IPFIX is not able to send data to the second collector which is configured and active
wi01092187	You may see a CP crash during 'show ip ospf lsdb vrfid xx' command during OSPF LSDB changes
wi01087180	FDB and ARP Learning not updated immediately if PC roams across ports, e.g. WAP when just using L3

©2013 Avaya Inc. Revision 01.02

	protocols.
wi01098132	Standby CP may crash if there are no neighbors learnt on the IGMP interface,
wi01066489	CP may core if many telnet connections initiate, are not cleaned-up, and then time-out
wi01085250	CP could core if the following situation: 1. enable pim-sm and fast leave 2. host 1 sends in include S1,S2,S3,S4,S5 for group x 3. host 2 sends an exclude S1,S2,S3,S4,S5 for group x 4. host 1 leaves group x
wi01088262	IP header checksum intermittently incorrect when IPFIX enabled and ACE remarking DSCP
wi01090547	Fan error will not be cleared if transient Fan error.
wi01091874	Pings fail to the local circuitless IP interface when created with 32-bit mask. E.g.: 1. Create Circuitless IP interface, say, 1.1.0.1/32 2. ping 1.1.0.1 then the ping failed.
wi01093136	Crash in IGMP after disabling PIM. During IGMP's cleanup process, it was possible for IGMP to free up memory containing a port structure, then later try to access it again. Problem was only seen for IGMPv3 interfaces.
wi01094476	Problem: Packets destined to egress VSP are sometimes incorrectly sent to the CP for processing. Packets arrive at the CP without requisite header pre-pended, resulting in bogus Warning log entries and non delivery of packet. CP1 [04/23/13 16:57:18.647] 0x00024750 00000000 GlobalRouter CPU WARNING CppRxFrames: Received a packet(s) with an Invalid LPID (1618) (total invalid LPID pkts now = 64122) The condition was caused by the following sequence of events: • Subnet x.x.x.x/n is present for local vlan • A set of ECMP routes exist for subnet x.x.x.x/n • Subnet x.x.x.x/n is removed when vlan goes down (i.e. last active port in vlan goes down) • ECMP routes becomes active. Traffic is still flowing. • When vlan comes back the Local subnet x.x.x.x/n is reinstalled causing the improper removal of the ECMP route and incomplete installation of local

	subnet. □ Invalid forwarding entry will result in broadcast traffic (ARP, ICMP request, etc.) not being forwarded out the local VLAN. Also MACs for hosts on that local VLAN will not be learned unless flows are initiated from the host first or ping initiated from the VSP ACLI. This results in some local hosts being reachable while others are not.
wi01095078	Fan failure LEDs may turn-on for 30 seconds or less during cold start of chassis.
wi01096850	If there are several telnets to VSP CLIs which are left around idle so they timeout, a timing issue may be hit when one of the CLIs timeout and attempt to close the CLI which causes a core.
wi01098169	Accessing ISIS configuration parameters when ISIS is disabled may cause a CP core.
wi01098430	If you create a vlan with ports on multiple line cards and non-default STG group, power down one of the line cards, add additional members to the vlan, then power up the line card, the ports from that card will not be member of the STG..
wi01077725	ARP table may not be displayed in "show tech"
wi01095411	ACLI doesn't show ethernet discard count incrementing which EDM does
wi01095911	Cooling Module Card Type/Module Desc.(9012 FC/SC/RC) are incorrect in show/fulltech output
wi01102646	Possible crash in tMainTask in function getFirstISAdjAreaInfo when unsupported ISIS MIBs are polled: isisSummAddrTable,isisISAdjAreaAddrTable, isisISAdjIPAddrTable and isisISAdjProtSuppTable.
wi01107702	The SPB BEB nodes can crash with the following signatures. ip_rtdeleteVrf: orec is NULL! RT:%ld.%ld.%ld.%ld Or plsbDeleteBmac: routeTree empty, non-zero count. This issue was caused by a recursive call made to the RTM for the same route. This can happen in the following scenario, * Alternative route feature is disabled in the GRT or VRF under consideration. * There is a network/route X that is learned via some

	routing protocol other that ISIS (RIP, OSPF, BGP, static, etc), * The same route is learned via SPB/ISIS. SPB will add that route to the RTM, and if ISIS_SPBM route is more preferred, will replace the existing route. * To replace the route, the RTM first deletes that existing "Best Route". This triggers a notification to other protocols to submit their "Best" Routes. * This trigger to ISIS/SPB, will cause ISIS/SPB to call RTM to add the same route again in a recursive manner, which can cause corruption of the RTM data structures. * The crash can occur, when next time the BEB tries to remove that route. For example, * Route 10.0.0.1 is learned and installed via OSPF. * Enable SPB, and ISIS learns 10.0.0.1 from remote BEB. * ISIS adds route 10.0.0.1 to RTM. * RTM now shows route 10.0.0.1 as ISIS route. * Disable ISIS, ISIS cleans up that route, encounters the above errors and crashes.

10. Outstanding Issues

Please see "*Virtual Services Platform 9000, Release Notes* release 3.3.0" (NN46250-401, 04.02) available at http://www.avaya.com/support for details regarding Known Issues.

In addition, the following issues have been identified:

ID	Problem Description	Workaround
wi00989121	When you upgrade the software image, a slight chance exists that one of the Switch Fabric or interface modules can fail to upgrade, which results in a rollback to the previous release.	After the upgrade, use the show system software command to verify that the upgrade was successful. If the upgrade was not successful, activate the Release 3.3.4 software again.

©2013 Avaya Inc. Revision 01.02

wi01082088	If you see this in your log file: CP2 [02/07/13 10:23:38.728] 0x000187e2 00000000 gnwt OSPF INFO HA-CPU LSDB sanity check: AS external checksum total mismatch. master value = 0x12aa89e ha-cpu value = 0x12b68b9	- Get show ip ospf ase off both CPs - Compare output o If self-originated LSAs then non-impacting reset the standby CP. o If any are not self-originated then contact customer support
wi01102999	Multicast MAC config might conflict with VLAN configuration such that VLAN does not get configured. If this occurs the following message will be logged: HW ERROR rarAllocateMgid: Group (4) already allocated! CP1 [05/26/13 12:27:53.488] 0x0002c676 00000000 GlobalRouter VLAN ERROR vlanCreateVirtualLan: Can't set McGrpId!	If you are going to configure static Multicast MACs, then when configuring VLANs, don't make the VLAN number consecutive, i.e. skip some numbers, e.g. 1,5,10, etc to allow Mcast mgids to be configured between the VLANs and avoid conflict.
wi01091558	Lifecycle Error "LifeCycle: ERROR: Cannot get create /opt/patch link patch"	This log can be ignored
wi01092093	Datapath lockup may occur when using packet filter with forward to nexthop action. Ingress datapath lockup occurs when a 319 byte packet destined to control plane (i.e. ARP entry ageout) matches a packet filter with redirect to nexthop action. Lockup affects all ports in slice. Slot needs to be reset to recover use of the slice.	Disable packet filter. Apply patch for 3.3.2.1 or upgrade to 3.4.0.0.
wi01097311	When there are 2 MLTs with ports on the same lane such that one MLT has LACP enabled on it and the other is Static MLT, atleast one port from each MLT is brought down, the static MLT ports port mask is not updated, thus you'd lose traffic on that Static MLT	Don't mix ports from different MLTs onto same lane if MLTs are a mix of Static and LACP.

11. Known Limitations

Please see "*Virtual Services Platform 9000, Release Notes* release 3.3.0" (NN46250-401, 04.02) available at http://www.avaya.com/support for details regarding Known Limitations.

MLT configuration recommendation:

MLT is designed for redundancy/robustness for when components/subsystems that comprise the network fail. To take advantage of this, it is suggested that MLT links span different IO cards so that if there is a failure on a card it only takes down one MLT link and the others continue to operate normally. If there are more MLT ports required on a single card, then those links should reside in different "slices" on a given card. A "slice" is a grouping of ports that are handled by a single forwarding engine on the IO card.

©2013 Avaya Inc. Revision 01.02

For 24x10G card, a “slice” is grouping of eight ports, and for 48x1G it is a grouping of 24 ports. For MLT links on the same 10G card, they should span different “slices”, or groups of eight ports, i.e. 1-8, 9-16, 17-24. For MLT links on the same 1G card, they should span different “slices”, or groups of 24 ports, i.e. 1-24, 25-48.

You may have to wait upto 30 seconds between subsequent“show pluggables” commands to give time for pluggable information to be refreshed.

New external flash devices come with a FAT16 format. While this appears to work correctly when inserted into a 9080CP card, there is an incompatibility issue when there are more than 169 log files created. The incompatibility will cause the logging mechanism to stop writing any new log files. To correct this issue you need to reformat any new flash device after it has been inserted into the 9080CP with the “dos-format” ACLI command as explained in the document: “CP Module Compact Flash Replacement”.

VSP 9000 Power Supply LEDs are in a non-deterministic state when the CP Power Supply indicator is lit RED indicating fault. There will be log messages indicating the Power Supply fault event but the PS LEDs may be RED, GREEN or OFF.

12. Documentation Corrections

For other known issues, please refer to the product release notes and technical documentation available from the Avaya Technical Support web site at: http://www.avaya.com/support .

Copyright © 2013 Avaya Inc - All Rights Reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Avaya.

To access more technical documentation, search our knowledge base, or open a service request online, please visit Avaya Technical Support on the web at: http://www.avaya.com/support