avaya.com

Virtual Services Platform 9000
Software Release 3.3.3

1. Release Summary

Release Date: April 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.3.3.3.0.tgz	Release 3.3.3.0 archived software distribution	105009506
VSP9K.3.3.3.0_modules.tgz	Release 3.3.3.0 Encryption Modules	39418

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.

Load activation procedure:

software add VSP9K.3.3.3.0.tgz
software add-modules 3.3.3.0.GA VSP9K.3.3.3.0_modules.tgz
software activate 3.3.3.0.GA

6. Version of Previous Release

Software Version 3.3.2 and 3.3.2.1

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 3.3.3

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
wi01053272	ip igmp static blocked port entry for a range of address does not filter all the entry, it only filter the first entry.
wi01074260	Loss of control traffic going to CP may be experienced due to a Catskill FIFO overflow condition if control traffic bandwidth exceeds CP limits for extended duration.
wi01075491, wi01085213, wi1067115, wi01088040	CP may core when many SSH sessions left un-terminated, when EDM sessions terminated or another SSH session started..
wi01054721	The QE lockup detection and recovery is done only 5 times on an IO module; after that, the IO module will need to be reset.
wi01081965	IO or SF card may not come-up if there are multiple SFs in system but none in SF1 or SF4 slot
wi01087211	After switch-over back-up CP may core before it comes-up.
wi01052127	When SPB decommissioned - any ISIS control packets received on the two vlans that were previously configured as BVLANs will not be forwarded on member ports of the VLANs as

	required. This issue does not impact any traffic on other VLANs.
wi01054618	When configuring SPBm, creating the vlans used as B-VLANs without first configuring them using the "b-vid" command under the "isis spbm" instance will cause the vlans to act as regular bridged vlans until the b-vid configuration is completed and may cause ISIS adjacencies not to form properly. – made change to not allow this configuration sequence.
wi01054685	When doing a HA failover on the BEBs that also have an IST configured and have a virtual BMAC configured, you may see ISIS errors in logs on both the new master and the new standby CP.
wi01064256	If terminate sshd while ssh sessions active, may cause a CP core.
wi01064557	With default route on VRF 1, hot insert of IO card reports "COP-SW ERROR" ercdAddEcmpDefaultRoute: Arp rcdRadixLookup failed" and "ercdProcArpRecMsg: Failed to Add Ecmp Default Route"
wi01065688	Telnet Session not timing out if password is not provided
wi01065919	Removed LACP ports still appear LACP tab in EDM
wi01067518	Unable to configure aggregate-address summary-only under BGP "aggregate" or "network" command.. The issue is related to invalid consistency check which doesn't allow the following forms, (1) xxx.255.yyy.zzz (2) xxx,yyy,255.zzz (3) xxx.yyy.zzzz.255
wi01067521	Configuring a blackhole route and importing it into BGP causes a crash in BGP.
wi01070934	CP Swap-out: The replacement Standby CP may have issues booting-up if the user does a "no sys power" on the Standby CP prior to pulling it out. In this case, the new Standby CP will core and reboot, thus taking longer to boot-up. Work-around is to not use the "no sys power" command for the standby CP that is to be removed. Instead reset the standby CP (e.g. "reset -y" on the standby CP or "slot reset <slot standby is in>" from the master CP). Then pull the standby while it's Online LED is blinking amber. Inserting a standby CP will now power up.
wi01070953	Small timing window which could cause core on CP after a switch-over. If an igmp packet (v3 membership report) arrived on the new master on VRF 0 right after switching from standby.
wi01071339	As the size of BGP RIB increases, so does the delay to get the cli prompt back when dumping show ip bgp route <prefix/len>..There is no delay ,when dumping show ip route

	<prefix/len> though. With RIB of size 40 K, the delay is about 16-20 seconds. With RIB of size about 400 K, the delay is longer than 120-140 seconds.
wi01076360	Core occurring on an IO card while performing ACL log processing. Core was caused by an invalid source port being associated with the incoming packet.
wi01080585	On chassis power-up, the following error log may be seen: "Failed to set software link scanning for Unit %d Port %d. ERROR !!!"
wi01080215	On chassis power-up, NFS mounting the intflash/extflash may fail if there were numerous CP power-downs while writing to Flash file-system
wi01082434	Continuous Invalid CPU_MAC_ETHERTYPE logs could fill the logfile
wi01084200	Default MAC flap detect loop protection mechanism could get triggered by intentional use of same MAC address by different servers, e.g. redundant firewalls.
wi01065701	VSP will allow the telnet connection from the block subnets to the point of showing the login screen.but not allow login.
wi01082697	Can't recover from ports that get shut-down due to Datapath Heartbeat time-outs.

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 3.3.2.1 software again.

wi01026336	In Release 3.2 and 3.3, there is a known issue that affects traffic flow for MLTs when two or more IO cards are reset. After the IO cards are up and operational and the ports are in “FORWARDING” state, traffic loss may happen for MLTs with port membership on these slots. If the slot has IST port members, the IST may not come up. This only affects configurations where there are multiple MSTP instances and there are MLTs configured. This problem does not occur if the switch is in RSTP mode or if there is only the default MSTP instance.	If at any time multiple cards need to be reset, do them one at a time. Wait until the first card is booted up completely and is in operational state before resetting (no sys power slot #) the second card. If one IO card reboots due to some fatal error, and a second card also reboots before the first one is up and operational, this problem may occur. If you are experiencing traffic loss after such an event, check the spanning tree port configuration using “show spanning-tree mstp msti port config” and make sure all expected ports are present. If ports are missing from the MSTIs, there are two possible workarounds that can be done: 1. Remove each of the missing ports from all VLANs and then add them back to each VLAN. This can be cumbersome if there are many VLANs and many missing ports. 2. If removing ports is not feasible, then a reboot is required to rectify the problem.
wi01052821	Configuring Egress Logging on a port that has remote mirroring on it will cause extra 8 bytes at the end of the packet. Also there is a chance of LANE lockup if both remote mirroring tunnel and logging is configured on a port.	Do not configure Egress Logging on the port that has remote mirroring on it. This port is the port which is connected to the remote via the tunnel.
wi01057618	Occasionally, the following error messages may show up on the console: IO6 [11/02/12 15:04:12.255] 0x00170563 00000000 GlobalRouter COP-SW ERROR K2-2 PCIE_BAD_ADR INT Event, bad address = 0x12fb8a6c IO6 [11/02/12 15:04:12.255] 0x00170566 00000000 GlobalRouter COP-SW WARNING K2-2 CMD PKT Logic Error: REPLY CODE=0x80 IO6 [11/02/12 15:04:12.255] 0x00170574 00000000 GlobalRouter COP-SW ERROR K2-2 Zag-1 BAP I/F Error Adr = 0x70, Data = 0x2000 IO6 [11/02/12 15:04:12.255] 0x00170574 00000000 GlobalRouter COP-SW ERROR K2-2 Zag-1 BAP I/F Error Adr = 0x74, Data = 0x20b8a6c IO6 [11/02/12 15:04:12.255] 0x001705fb 00000000 GlobalRouter COP-SW ERROR K2-2 Zag-1 BAP RSP reg 0x1C: 0x402 0xD4: 0x10 0xD8: 0x20b8a6c IO6 [11/02/12 15:04:12.255] 0x00118526 00000000 GlobalRouter COP-SW ERROR @/vob/cb/nd_dld/cbio/rlcd/lib/rlcd_util.c#574:rspRead32() k2b_pci_read failed rc: -1!!, k2DevId: 6, k2Slice: 2	These messages will not impact the operation of the switch and can be ignored

wi01082088	wi01082088 HA-CPU LSDB sanity check: AS external checksum total mismatch	- 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

wi01088262	Calculating intermittent incorrect IP header checksum when IPFIX enabled and ACL ACE remarking DSCP	
wi01085453	IPFIX is not able to send data to the second collector which is configured and active	
wi01091558	Lifecycle Error "LifeCycle: ERROR: Cannot get create /opt/patch link patch"	This log can be ignored

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 the card. A "slice" is a grouping of ports that are handled by a single forwarding engine on the IO card.

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.

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 .

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