Virtual Services Platform 9000
Software Release 3.3.2.1

1. Release Summary

Release Date: February 7, 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.3.3.2.1.tgz	Release 3.3.2.1 archived software distribution	104979981
VSP9K.3.3.2.1_modules.tgz	Release 3.3.2.1 Encryption Modules	39421

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.3.3.2.1.tgz
software add-modules 3.3.2.1.GA VSP9K.3.3.2.1_modules.tgz
software activate 3.3.2.1.GA

6. Version of Previous Release
Software Version 3.3.1.1 and 3.3.2

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 is recommended to fully interoperate with ERS 8800 7.2 SPBm network deployment.

8. Changes in 3.3.2.1

New Features in This Release

       o   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
wi01048245	A CP core may occur when connecting from a telnet after maximum number of telnets reached then disabling and enabling the telnet service
wi01052613	An CP core may occur when executing the 'show ip mroute route' command of the source mask changes for the SGRPT prune entry
wi01052801	An IO core may occur while making dynamic config changes to ip arp static-mcast
wi01054721	VSP 9000 loop-detect/MAC-Flap features are erroneously shutting down ports when packets with source MAC address of zero are received on different ports. VSP 9000 should not be tracking these packets
wi01055410	A very small memory leak would happen when ports bounce. It would take about a month of a port constantly bouncing at a high frequency to run out of memory on standby CP, then it would core and reboot.
wi01058570	IPFix templates are not exported to the IP collector
Wi01058573	LSM packet loss may cause invalid dropping or forwarding of packets.
wi01058584	Inserting an SNMP notify filter using EDM may result in a CP Core
wi01059666	An CP core will occur if a BGP Update message with an AS path attribute whose length extension bit is set even though the contained data length is less than 255 is received
wi01063456	A CP core may occur when running the ACLI command 'show isis spbm multicast-fib summary'

wi01063477	A small memory leak is triggered by save config, an image sync or add/activate software activities. It would take about 25 years of normal save config activity to run out of memory
wi01065688	Telnet to the VSP9K will not time-out when at the username/passwd prompt
wi01069452	Configuring a black hole route and having BGP distribute it causes a crash in BGP (on the CP)
wi01069455	Unable to configure aggregate-address summary-only under BGP. This is only seen with routes containing an octet of 255 in other than the 1st octet.

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.

wi01051864	The "show ip mroute next-hop" command may not display properly after a CP failover.	Use the command "show ip pim mroute" to view multicast routing information.
wi01052127	If SPB is de-commissioned after being previously configured on the switch, 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.	There are three possible workarounds: Do not use the two VLANs to carry ISIS traffic after de-commissioning SPB; OR do not use the two VLANs after de-commissioning SPB; OR reset the line cards where ISIS control packets on the two vlans are ingressing the switch.
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.
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.	The "b-vid" under the SPBm instance must be configured before the BVLANs are created.
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

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.	Don't 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.

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 .