avaya.com

Virtual Services Platform 9000
Software Release 3.3.2.0

1. Release Summary

Release Date: November 19, 2012
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.3.3.2.0.tgz	Release 3.3.2.0 archived software distribution	104986634
VSP9K.3.3.2.0_modules.tgz	Release 3.3.2.0 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.3.3.2.0.tgz
software add-modules 3.3.2.0.GA VSP9K.3.3.2.0_modules.tgz
software activate 3.3.2.0.GA

6. Version of Previous Release

Software Version 3.3.1.0 and 3.3.1.1

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

8. Changes in 3.3.2.0

New Features in This Release

- There have been some enhancements in this release to add resiliency and help with troubleshooting. Some of these are:
  - Improved intelligence in module failure scenarios to recover the module before determining that it must be powered down
  - Improved intelligence when Datapath Heartbeat messages occur to shut down port in certain scenarios – see wi01044322 under Problems Resolved in this release for more information
  - More accurate fan failure reporting
  - Improved error logs if an error occurs when powering up modules
  - Improved error logs and recovery techniques for certain module hardware errors

Old Features Removed From This Release

The following DOS rules have been disabled in VSP 9k:

IPv4 packets with SIP equal to DIP
IPv6 packets with SIP equal to DIP
TCP packets with control flags of 0 and sequence number of zero

Problems Resolved in This Release

ID	Problem Description
wi01016629	DHCP relay entries configured on multiple VRF's are not synchronized correctly to the standby CP, so after a failover they are no longer part of the running configuration
wi01020503	The Switch Fabric may core during a CP switchover due to a timing error
wi01021309	After a failover to the standby CP, the system power supply status is not displayed correctly
wi01024351	IP Multicast traffic is not flooded over SPB L2VSNs
wi01024358	SPB multicast entries from an ERS switch with Multicast over SPBm enabled are not generated on VSP 9K switch
wi01024867	IP packets classified as IP shortcut are not handled properly if they are routed into a

	loop
wi01026692	Executing the "show isis spbm multicast-fib i-sid" command may result in a core
wi01028276	A default route re-distributed from a VRF to Global Router can conflict with the RSMLT temporary default route during an IST node reboot. This will cause traffic using the default route to be sent to a stale next hop.
wi01029890	Unable to apply route policy to redistributed routes from one VRF to another VRF.
wi01031565	Black holing of traffic can be observed when the lowest numbered IST port between two VSP switches is brought down for some reason. The problem is typically triggered when all local LACP ports in an SMLT configuration are down and the traffic is forced over the IST to reach the operational SMLT port on the other switch. When this occurs and the lowest numbered IST port on the local switch is down, the traffic may not reach the destination because it is dropped by the switch.
wi01032865	SPBm connectivity issues will occur when there are greater than 9 peer BEBs in an L3VSN
wi01033092/ wi01042348	10GbLRM SFP+ is not being detected after removing and re-inserting into the 9024XL blade.
wi01034189	If VRRP is configured on many ports, there is a possibility that the VSP may attempt to send VRRP advertisements for more than one port at the exact same time causing a buffer corruption and the advertisement(s) not to be sent. When this error occurs, you may see one or both of the following log messages: 0x00000655 00000000 GlobalRouter SW ERROR Invalid cardType detected (0xX) for lpid 0xY - getLpidFromPhyPort!! 0x000005fe 00000000 GlobalRouter SW ERROR Invalid phy port: XXX detected in getLpidFromPhyPort conversion!!!
wi01034276	If Egress Filters are configured with the log action, packets matching the filter rule will be truncated upon egress of the port
wi01034513	If the RIP supply and/or RIP listen attributes are disabled, they will be re-enabled after saving the configuration and rebooting the VSP instead of remaining disabled.
wi01035347	The following error message can be seen on a running system: GlobalRouter KHI ERROR Could not read /proc/2206". It is the result of a KHI polling error and has no functional impact.
wi01036045	A BGP advertisement message with path attributes larger than 260 bytes will cause a CP crash
wi01036961	Ping and traceroute from a non Global Router VRF will fail to local subnet destinations
wi01037979	InterVRF Route Redistribution policy configuration for BGP will be lost after the second CP failover. The interVRF redistribution policy would need to be reconfigured.
wi01039021	In some cases, egress traffic gets blocked at the traffic adapter. Software will detect this condition and recover from this automatically
wi01039834	After several power cycles of an IO module, the power reporting get corrupted and will not power on the module
wi01040935	"show ip route count-summary" and any command that uses it, such as "show fulltech," will result in a core if a blackhole route is found in the route table before any non-blackhole route, for example if the default route is a blackhole.
wi01041317	After inserting a new standby CP module that is running the same version of software on the master CP into a live system, the encryption modules are not synched to the new standby CP
wi01041403	No LACP trap is generated when an lacp link goes down on the VSP. This makes it hard to determine which link brought down the SMLT when there is an lacp-based MLT on an IST peer. This is fixed by adding a log message, not a trap, upon a link state change:

	LACP INFO Aggregation Link State Change (mltid = 3,link state = Local/Remote down/up)
wi01041566	The "show isis spbm ip-unicast-fib" command does not display VRF (L3VSN) fib entries
wi01041721	An IST link configured using EDM will not become operational
wi01042553	The special encapsulation of the ARP packets going over the IST is not removed when the destination MAC address is unknown. Also, the packets were being sent on port 3/1.
wi01042969	OSPF INFO HA-CPU LSDB sanity check: AS external checksum total mismatch log message is changed from Warning to Info. This message indicates an internal error condition of a record, but has no functional impact, and OSPF will operate correctly if an HA failover is performed.
wi01044014	Executing the "show filter acl" command on CP modules (ex 1/1 and 2/1) will hang the console window
wi01044322	The VSP9000 injects special Heartbeat packets into the data path periodically to help confirm the data path is functioning. These packets will loop through each subsystem on the line card and return to the system processor. If 4 packets in a row are delayed or blocked, a data path heartbeat error is reported and an alarm is set. Such errors are an indication of a serious enough problem that the ports associated with that path will be shut down and system redundancies will divert traffic. When a port has been shut down, the port state reason code will be set to DP HEARTBEAT. CLI command “show interfaces gigabitEthernet state” will indicate the port shutdown reason. Once data path heartbeats recover, ports will be allowed to come up if “auto-recover-port” is enabled for that port. If not enabled, the ports can be allowed to come up by disabling and re-enabling the port via CLI command “shut” followed by “no shut”. If for any reason it is undesirable to shut down ports in the system due to data path heartbeat failures, this aspect of the feature can be disabled box wide with the CLI command “no sys data-path-fault-shutdown”. This feature is enabled by default. Auto-recovery is disabled by default.
wi01044654	With an NLB server and another device both connected through the same switch to the VSP, IP connectivity cannot be established between the device and the NLB virtual address
wi01044690	SPBm connectivity issues with ISIS adjacencies may occur when SMLT disabled and re-enabled
wi01045789	If the VLACP timeout is mismatched between the VSP and the device at the other end of the link, power cycling the standby CP module will cause VLACP to bounce.
wi01046688	If a patch is applied on a system without a standby CP, the patch will take 5 minutes to commit
wi01047805	For ARP responses coming over the SMLT links, VSP 9k adds special encapsulation and sends those over the IST link to the other peer. The IST peer is supposed to process this packet and forward only if needed. For some specific IST MLT IDs, the packets were looped back on the SMLT link and the packets grew by 4 bytes.
wi01048072	When ACLI is used to configure an ospf area range for area 0.0.0.0, the area range definition will not be saved to the configuration file
wi01048359	Statistic records of 128 bytes are not removed properly when an IGMP leave is received in the linecard. Over time, this can lead to an out of memory condition on the linecard.
wi01048636	Host names are appended with extra character when executing the "show isis lsdb tlv<tlvid> detail" command
wi01050620	In order to support fast failover SMLT protocol, each device broadcast its own port

	states to its IST peer device through IST port continuously. When the device detects the SMLT ports on its IST peer device has gone down by either receiving the LSM with port down info or missing 3 consecutive LSM messages for its peer, it starts to forward traffic on behalf of its peer device. In SMLT deployments where the SMLT links are operating at 1G speed, VSP 9000 could potentially introduce a loop. Since IST ports are on 10G interfaces, there are chances that LSM packets from the IST peer device as a burst. Then, the burst of LSM packets will be forwarded by the switch fabric to the egress ports. However, there will be momentary congestion and it will cause the LSM packets dropped by the egress FIFO. Due to the drop of LSM packets from its peer, it will start to forward traffic on behalf of its peer while its peer's SMLT port still up and forwarding traffic
wi01050795	When the last IGMP or PIM leave is received on a VLAN, the VLAN multicast record of 236 bytes is not removed properly. Over time, this can lead to an out of memory condition on the CP.
wi01051793	ISIS packets are consumed by the VSP even though SPBM is not configured
wi01051819	A PIM Assert with a null value for upstream neighbor causes a CP crash and failover to the standby CP.
wi01051889	Lifecycle recovery menu should be brought up if internal flash is corrupted in order to reformat the internal flash
wi01052062	ISIS adjacencies will not come up if BVLANs are created after SPBm NNI Interfaces are configured

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 3.3.2.0 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.
wi01052749	IPFix Templates are not exported to the IP collector	None
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.
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	Apply ingress filters to drop packets and unlock port that was shutdown
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

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 .