Virtual Services Platform 9000
Software Release 3.4.2.0

1. Release Summary

Release Date: June 3, 2014
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 3.4.0.2 (NN46250-401, 05.04) 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.3.4.2.0.tgz	Release 3.4.2.0 archived software distribution	114709936
VSP9K.3.4.2.0_modules.tgz	Release 3.4.2.0 Encryption Modules	41891

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.3.4.2.0.tgz
software add-modules 3.4.2.0.GA VSP9K.3.4.2.0_modules.tgz
software activate 3.4.2.0.GA
```

6. Version of Previous Release

Software Version 3.4.0.2, 3.4.1.0

7. Compatibility

N/A

8. Changes in 3.4.2.0

New Features in This Release

None.

Old Features Removed From This Release

No features removed from this release.

Problems Resolved in This Release

ID	Description
wi01126456	While processing an IGMPv3 report if any group record requested is being filtered the entire packet is ignored.
wi01135195	“show filter acl log” does not allow multiple port input as documentation states. show filter acl log {slot/port[-slot/port][,...]} [<1–2048>] [<1–2000>]
wi01148937, wi01155621	Consistency check added to restrict configuration of ISIS to 64 interfaces.
wi01149668	Messages when running “flight-recorder all’ are misleading. Fix adds following messages to indicate that the trace and snapshot files are in the archive file and deleted: NOTE: Deleting Flight-recorder trace files (if any) from /intflash/flrec/#/ and adding them to the archive NOTE: Deleting Flight-recorder snapshot files (if any) from /intflash/PMEM/#/ and adding them to the archive
wi01149844	Configuration of "rvs-path-chk mode strict" reverts back to disabled after VSP reset/reboot. Fix saves to configuration file.

wi01150183	Modifying ECMP max-path of a VRF does not get set.
wi01150587	VSP9000 CP may reset when applying access policies from a CLI session using telnet.
wi01150933	Invalid SSH connection attempt passes banner when RADIUS authentication is enabled. Fix prevents the banner from being sent for invalid connection attempt.
wi01151197	L2traceroute does not work if CFM is enabled before SPB enabled.
wi01151199	CP may reset while running “show isis spbm i-sid all” on scaled SPB systems with long interface names.
wi01151724	CP may reset when a default route with mask less than 8 bits goes unreachable.
wi01151834	CP may reset when a successful SSH session connection is made immediately after many failed SSH session connections. Probability of reset increases when device is under DOS attack with invalid SSH session requests.
wi01152214	Not able to access EDM via Firefox Version 27. Firefox 27 extends cipher which is not supported without the encryption module loaded. Fix on box EDM to not extend encryption option for non-loaded cipher.
wi01153264	CP may reset when TACACS+ server is deleted while two or more authentications are outstanding.
wi01153266	Soft restart of individual BGP peers in VRF does not work.
wi01153269	When a port in the MLT is admin down, the mstp port state stays always Forwarding which results in removing the admin down port from the MLT and causing all other ports in the MLT to go Discarding.
wi01155324	“rvs-path-chk” configuration should be reset to default values when the IP address on the interface is deleted and recreated.
wi01155329	CP may reset because of TACACS/CLI multi-thread unsafe data access
wi01155340	Multicast stream with TTL=0 was forwarded. Should be dropped.
wi01155960	Parity error detected at ingress MAC causes invalid packets to be broadcast to undesired slots to all slots in a VSP cluster. IST outage and non-deterministic behavior maybe observed. The fix drops these packets and also changes the ERROR message to a new ALARM message. EventId: 0x001205eb AlarmId: 0x04800001 Terse msg: BCMSDK unit = %d, L2X, entry %d parity error

	Probable cause: "HW parity error detected in BCM Scorpion MAC" Remedy: "Hardware failure that can only be cleared via slot reset. Please reset the slot as soon as possible" Change also added this alarm message for SPI ROM loading error condition. EventCode: 0x001205ed AlarmId: 0x04800002 Terse msg: BCMSDK %d: p=%d SPI-ROM load didn't complete (0x%x) Probable cause: "SPI ROM load did not complete" Remedy: "Hardware failure that can only be cleared via slot reset. Please reset the slot as soon as possible"
wi01156194	A chassis with 7 or more IO slots populated may experience cbBcm_QeEgressLockupWorkaround events and false ZAGROS lockup events on multiple slots, slices and lanes during chassis power cycle.
wi01156249	Memory leak observed when sending TACACS_AUTHENTICATION_FAILURE and TACACS_RX_UNSUPPORTED_FRAME traps.
wi01158685	"show khi cpp port-statistics" command does not correctly show raw Tx SLPP packet counts.
wi01159274	Add support for recognizing new devices via SONMP: mVSP8284XSQ(213), -- Virtual Services Platform 8284XSQ mERS3549GTS(214), -- Ethernet Routing Switch 3549GTS mERS3549GTS-PWR-PLUS(215), -- Ethernet Routing Switch 3549GTS-PWR-PLUS mVSP4950GSX-PWR-PLUS(216), -- Virtual Services Platform 4950 GSX-PWR+ mVSP7024XT(217) -- Virtual Services Platform 7024XT
wi01159779	ISIS adjacency timeout occurs prematurely after frequent NNI interface UP/DOWN transitions.
wi01160319, wi01160328	CP resets when SNMP get of ISIS Unicast or Multicast FIB table causes watchdog condition. CP may also reset during VPFM discovery when performing 'rcIsisPlsbUcastFibEntryNext' MIB get. These exceptions occur when OutgoingPort name string (concatenation of all outgoing interfaces names) is longer than 255 characters. Fix truncates OutgoingPort name returned with MIB to 255 characters and end string with "…" to indicate truncation of name.
wi01160415	BGP Robustness Issues Addressed - BGP routes not installed in non GRT VRF with 4 BYTE AS Enabled - Invalid BGP path attribute is sent causing peering to go down when "remove-private-as" is enabled and VSP receives routes with private AS and 4 Byte AS enabled. - BGP peer is sending open message with My AS:23456 (Trans-AS) when the peer is upgraded to AS-4byte, which is causing AS mismatch ,though the AS numbers of both the peers are in AS-2-byte range - EBGP session goes down with "Update Error: Unrecog-Wellknown-Attrib" when AS set has

	more than 70 AS and routes are advertised to another EBGP peer, while 4 Byte AS is enabled. - EBGP peer between a VSP supporting 4 Byte AS and 2 Byte AS to a VSP that is 4 Byte AS enabled causes the peering to go down with Update Error: Malformed-ASPath. - EBGP peer between VSP aggregating routes from 2 Byte AS to 4 Byte AS peer sends invalid update to BGP peer. - EBGP peer between VSP 4 Byte AS and 2 Byte AS Peer may cause reset if AS path length is longer than 255. - When 4 Byte AS enabled and BGP routes are aggregated as "as-set summary-only", the BGP peer sessions will go down with "Update Error: Malformed-ASPath" - After changing/deleting the specific remote-as for an individual neighbor that is part of a BGP peer-group. The remote-as is not set to the peer-group remote-as setting. - BGP neighbor route counts may be wrong. - show ip bgp route does not work on other VRFs if Global router BGP is disabled - Peer-group password was not encrypted. - Adding peer to peer-group does not inherit all the peer-group attributes. - A VRF does not advertise the routes that were redistributed from the GRT after disabling auto-summary.
wi01160645	Change log event message IO6 [02/10/14 15:15:25.198] 0x0011851f 00000000 GlobalRouter COP-SW ERROR ***** RSP Microcode Download Failed !!! for devId: 0 ***** To an ALARM EventCode: 0x0011851f AlarmId: <0x04600001> AlarmStatus: <ALARM_SET> ModuleName: <RMOD_RLCD> Severity: <S_ERROR> TerseMsg: <"***** RSP Microcode Download Failed !!! for devId: %-2d *****"> ProbableCause: <"The network processor loader cannot complete the microcode loading process."> Remedy: <"Reset IO module to clear the error. If problem persists, shut affected ports to minimize bad traffic and contact customer support."> The new alarm text is as follows, "***** RSP Microcode Download Failed !!! for devId:<rsp_id> *****" We introduce a new event-code as follows for alarm clear purpose. EventCode: 0x00118546 AlarmId: <0x04600001> AlarmStatus: <ALARM_CLEAR> ModuleName: <RMOD_RLCD> Severity: <S_INFO>

	TerseMsg: <"Slot %s down, clear previous RSP microcode alarm for devId: %-2d"> ProbableCause: <"Slot went down"> Remedy: <"No action required">
wi01160808	ip mroute next-hop entries not cleaned up properly when an IGMP leave is received for a multicast stream ingressing via SPB cloud.
wi01163095	Show ip route may cause CP reset if sys-name is greater than 18 bytes long.
wi01164616	4byte BGP AS peer-ship between two peers goes down when remove-privateAS and aggregate enable is enabled on the advertising router. The issue happens when the BGP Full internet routes are being injected into the FIB via ISP connection.
wi01166659	SSL related robustness improvement. Graceful discard of unknown packet type.
wi01166668	An update packet from the 4byte AS IBGP peer causes the session to be brought down with Bad-AS-Peer message. The issue is seen with full internet routes brought in via ISP and aggregation is enabled.
wi01166672	VSP9000 resets connection while parsing the capabilities. The BGP peer has these configuration settings: BGP global: route-refresh At BGP peer level route-refresh address-family ipv6 address-family vpn4

10. Outstanding Issues

Please see "*Virtual Services Platform 9000, Release Notes* release 3.4.0.2" (NN46250-401, 05.04) available at http://www.avaya.com/support for details regarding Known Issues.

In addition, the following issues have been identified:

ID	Problem Description	Workaround
wi01133152	When port membership of an MLT is changed the MSTP spanning tree state is enabled for the MLT regardless of its previous state. That is, configure for any port in the mlt no spanning-tree mstp force-port-state enable and show spanning-tree mstp port role shows spanning tree disabled and port state forwarding for each port in the mlt. Now add a port to the mlt, or delete one. show spanning-tree mstp port role spanning tree is now enabled for each port in the mlt.	Delete MLT member ports from the MLT and re-add the MLT member ports back to the MLT
wi01134134	ACL filter "default" deny action with "permit" control-packet-action not working after line card power off/on.	Once in the bad state, simply re-keying in "filter acl set 30 default-action deny control-packet-action permit" restores the functionality.
wi01135592	When ip mroute stats is enable via EDM, "PktsPerSecond" count is always showing zero.	Display properly by performing "**show ip mroute stats**" on ACLI.
wi01136699	syslog with ip-header-type circuitless-ip not working.	Use syslog with the default management interface ip address.
wi01152560	ISIS adjacency over the IST port comes down and does not get re-established automatically when the IST is deconfigured.	The configuration of SMLT peer-system-id and SMLT virtual BMAC is tied to having a valid IST configuration on the switch. Deletion of IST on a switch running SPBM is a service impacting operation and the following procedure must be followed when doing so. • Disable ISIS • Clear the SMLT peer system-id • Clear the SMLT Virtual BMAC • Delete the IST peer configuration • Enable ISIS and

		• Bounce the ports that are/were part of the IST MLT. Here is an example session output following this procedure. /* disable ISIS */ CB15:1(config)#no router isis enable WARNING:Disable ISIS will cause traffic disruption Do you want to continue (y/n) ? y /* Clear the SMLT peer system-id */ CB15:1(config)#router isis CB15:1(config-isis)#spbm 1 smlt-peer-system-id 0000.0000.0000 /* Clear the SMLT Virtual BMAC */ CB15:1(config-isis)#spbm 1 smlt-virtual-bmac 0x00:0x00:0x00:0x00:0x00:0x00 CB15:1(config-isis)#exit /* delete IST peer configuration */ CB15:1(config)#interface mlt 2 CB15:1(config-mlt)#no ist enable WARNING : Disabling IST may cause loop in the network! Do you really want go DISABLE IST (y/n) ? y CB15:1(config-mlt)#no ist peer-ip CB15:1(config-mlt)#exit /* enable isis */ CB15:1(config)#router isis enable /* At this point, the interface still needs to be bounced */ CB15:1(config)#interface gigabitEthernet 10/17 CB15:1(config-if)#shut CB15:1(config-if)#no shut

11. Known Limitations

Please see "*Virtual Services Platform 9000, Release Notes* release 3.4.0.2" (NN46250-401, 05.04) 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.

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 up to 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.

IPFIX is not supported on ISIS interfaces. Log messages such as the following will start filling up the log files:

```
IO3  [10/25/13 13:58:50.722] 0x0001c68d 00000000 GlobalRouter HW ERROR getSlotIdFromLpid: LPID
(2868) is not associated with a slot!
IO3  [10/25/13 14:02:30.791] 0x000005e0 00000000 GlobalRouter SW ERROR Invalid LPID: 2904 for
getPimPortFromLpid conversion!!!
```

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 .

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