

Virtual Services Platform 9000 Software Release 3.4.5.0

1. Release Summary

Release Date: January 2015

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.3.4.5.0.tgz	Release 3.4.5.0 archived software distribution	114811626
VSP9K.3.4.5.0_modules.tgz	Release 3.4.5.0 Encryption Modules	41894
VSP9K.3.4.5.0_mib.zip	Archive of all MIB files	772088
VSP9K.3.4.5.0_mib.txt	MIB file	4854520
VSP9K.3.4.5.0_mib_sup.txt	MIB file	817795
VSP9000v340_HELP_EDM_gzip.zip	EDM Help file	4012849
VSP9000v3.4.3.0.zip	EDM plug-in for v3430/vsp9000, built on 8/5/14, based on svn #31565	5627960
VSP9K.3.4.5.0.md5	MD5 Checksums	452

Note about image download:

Ensure images are downloaded using the binary file transfer. Perform MD5 checksum check on downloaded files to ensure file integrity.

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.3.4.5.0.tgz
software add-modules 3.4.5.0.GA VSP9K.3.4.5.0_modules.tgz
software activate 3.4.5.0.GA
```

6. Version of Previous Release

Software Version 3.4.0.2, 3.4.1.0, 3.4.2.0, 3.4.2.1, 3.4.2.2, 3.4.3.0, 3.4.4.0

7. Compatibility

8. Changes in 3.4.5.0

New Features in This Release

Old Features Removed From This Release

Problems Resolved in This Release

ID	Description
wi01146781, wi01190842	<p>Periodic non-impacting event causes the following message. 0x0017056e 00000000 GlobalRouter COP-SW ERROR K2-1 Zag-0 PMM Error Ext Adr = 0x1010, Data = 0x80000004</p> <p>Message is removed and converted into the following counter.</p> <p>"PMM FP PLEN Err" row added to the below output. SUSTDEV-VSP3:1(config)#show khi forwarding zagros 10</p> <pre> ===== ===== Forwarding KHI Details - Zagros Statistics - Slot 10 ===== ===== Health Indicator Ports 1-12 Ports 25-36 ----- K2 If 1->Zagros 171283 171095 Zagros->RSP 2548742 2548627 Zagros->QE If 1 183089 182903 QE If 1->Zagros 2428220 2378200 Zagros->K2 If 1 1260 534 ZAP Tx Ctl 4296888 4292936 ZAP Tx Data 49365 0 ZAP Rx Ctl 4296891 4292939 ZAP Tx HBE 2377051 2377123 PMM output Drop count 2365789 2365859 PMM Admission RSP 2365789 2365859 Drop Count 2365789 2365859 PMM RSP rx count 2548742 2548627 PMM RSP tx count 184349 183437 PMM HAB bus rx 2548742 2548627 PMM CIF request count 2377051 2377123 PMM CIF response count 2377051 2377123 PMM FP PLEN Err 1 0 PMM RSP PLC Threshold 170 170 PMM RE PLC Threshold 48 48 PMM Free Page Count (OPA) 16 17 PMM Free Page Count (RPA) 18 16 PMM Free Page Count (FPM) 2009 2010 PMM RSP PLC Packet Count 3^ 0 3^ 0 PMM Egress OOB 3^ 0 3^ 0 PMM Ingress Heartbeat 1^ 0 1^ 0 PMM Ingress COP Insertion 2^ 0 1^ 0 PMM Egress L2BC/UC 1^ 0 0^ 0 PMM number of pools 9 9 ----- Health Indicator Ports 13-24 Ports 37-48 ----- K2 If 1->Zagros 171096 171551 Zagros->RSP 2548591 2549121 Zagros->QE If 1 182903 183358 </pre>

	<pre> QE If 1->Zagros 2378165 2378693 Zagros->K2 If 1 535 988 ZAP Tx Ctl 4184309 4189216 ZAP Rx Ctl 4184312 4189219 ZAP Tx HBE 2377086 2377161 PMM output Drop count 2365823 2365898 PMM Admission RSP Drop Count 2365823 2365898 PMM RSP rx count 2548591 2549121 PMM RSP tx count 183438 184346 PMM HAB bus rx 2548591 2549121 PMM CIF request count 2377086 2377161 PMM CIF response count 2377086 2377161 PMM FP PLEN Err 2 3 PMM RSP PLC Threshold 170 170 PMM RE PLC Threshold 48 48 PMM Free Page Count (OPA) 16 16 PMM Free Page Count (RPA) 16 17 PMM Free Page Count (FPM) 2011 2010 PMM RSP PLC Packet Count 3^ 0 3^ 0 PMM Egress OOB 3^ 0 3^ 0 PMM Ingress Heartbeat 1^ 0 1^ 0 PMM Ingress COP Insertion 1^ 0 1^ 0 PMM Egress L2BC/UC 0^ 0 1^ 0 PMM number of pools 9 9 </pre>
wi01194312	<p>Allow the creation of a core file as option while requesting reset.</p> <pre> reset -coredump config t > sys action cpu-switch-over -coredump </pre> <p>These commands will cause the collection of core dump</p>
wi01194579	Add fixes for SSL vulnerabilities CVE-2014-3566 (POODLE) and 3568
wi01196467	<p>show debug spbm isis inode may cause CP reset with following backtrace.</p> <p>Lifecycle Crash Reporter: Process Name: cbc-p-main.x, Thread Name: tShell-cli, Signal 11, Slot: 2, PID 2514, LWP: 2983</p> <pre> [bt] Execution path: [bt] /opt/appfs/lib/cp/liblc_shm.so.1(_Z26lc_crash_exception_handleriP7siginfoPv+0xf4) [0xfadd22c] [bt] /opt/appfs/lib/cp/libee_infrastructure.so.1(ee_sigaction_dispatcher+0x47c) [0xe246dac] [bt] [0x100350] [bt] cbc-p-main.x(dumpIisisInode+0x3ac) [0x112949f4] [bt] /opt/appfs/lib/cp/libisis.so.1(cliDumpIisisInode+0x24) [0xf912fb8] [bt] cbc-p-main.x(execshowdebugspbmisisFunc+0xf4) [0x10a5cb98] [bt] cbc-p-main.x() [0x109fdc60] </pre>

	<pre>[bt] cbcplib-main.x(nncli_executeTree+0x404) [0x109fcb48] [bt] cbcplib-main.x(nncli_executeTree+0x3e8) [0x109fcb2c] [bt] cbcplib-main.x(nncli_executeTree+0x3e8) [0x109fcb2c] [bt] cbcplib-main.x(nncli_executeTree+0x3e8) [0x109fcb2c] [bt] cbcplib-main.x(nncli_execute_line+0xcc) [0x109fcee8] [bt] cbcplib-main.x(nncli_execute_cli+0x49c) [0x109fd430] [bt] cbcplib-main.x(start_nncli+0x34c) [0x109e2cec] [bt] /opt/appfs/lib/cp/libv2l.so.1(task_wrapper+0x278) [0xe96d8bc] [bt] cbcplib-main.x(ckrmThreadStarter+0x68c) [0x1132a37c] [bt] /opt/appfs/lib/cp/libee_infrastructure.so.1(ee_thread_create_start_routine+0x100) [0xe248f60] [bt] /lib/libpthread.so.0(+0x6844) [0xe90d844] [bt] /lib/libc.so.6(clone+0x84) [0xe44d518]</pre>
wi01198665	Show commands that display port MAC addresses may display wrong MAC values.
wi01198679	Set maximum 1024 dhcp forward-paths per vrf and maximum 1024 per chassis.
wi01199170	SMLT peer ARP entry incorrectly pointing to IST during SMLT failover/recovery
wi01199639	IO module may reset during Multicast record deletion.
wi01200326	traceroute to a local IP address from the local ACLI session will cause corruption of control plane data and errant forwarding of outbound packets from management applications such as telnet/ftp/traceroute.
wi01201767, wi01199363	While deleting a vlan in a VRF context, stale ARP discard entries may remain in the hardware datapath. If that subnet becomes reachable via OSPF, RIP, VRRP, etc, the IP address contained in the stale ARP discard record will prevent the forwarding of traffic for that IP address.
wi01204138	Successive syslog messages caused by BCM SDK events are not suppressed properly to a configured syslog server.
wi01202518	Some ARP Entries learned over an NNI link with a VSP7000 IST peer are not aging out properly after the VSP7000 has been isolated for more than 20 minutes. "show ip arp" shows dynamic entries with no port or tunnel name present.
wi01205121	"show ip arp vlan" erroneously displays 0/1 or 1/1 string for PORT

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	<p>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</p> <pre>no spanning-tree mstp force-port-state enable</pre> <p>and</p> <pre>show spanning-tree mstp port role</pre> <p>shows spanning tree disabled and port state forwarding for each port in the mlt. Now add a port to the mlt, or delete one.</p> <pre>show spanning-tree mstp port role</pre> <p>spanning tree is now enabled for each port in the mlt.</p>	<p>Delete MLT member ports from the MLT and re-add the MLT member ports back to the MLT</p>
wi01134134	<p>ACL filter “default” deny action with “permit” control-packet-action not working after line card power off/on.</p>	<p>Once in the bad state, simply re-keying in</p> <pre>“filter acl set 30 default-action deny control-packet-action permit”</pre> <p>restores the functionality.</p>
wi01135592	<p>When ip mroute stats is enable via EDM, “PktsPerSecond” count is always showing zero.</p>	<p>Display properly by performing "show ip mroute stats" on ACLI.</p>
wi01136699	<p>syslog with ip-header-type circuitless-ip not working.</p>	<p>Use syslog with the default management interface ip address.</p>
wi01152560	<p>ISIS adjacency over the IST port comes down and does not get re-established automatically when the IST is deconfigured.</p>	<p>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.</p> <ul style="list-style-type: none"> • 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
    
```

wi01192436	MLT up/down trap is not sent when first port of the MLT transitions up or last port of the MLT transitions down.	Log messages of the MLT up and down events are written and sent to syslog servers if configured.
wi01203279	SSH clone session option is not supported. Using clone session option in SecureCRT for SSH may cause system reset.	Do not use SSH clone session option.
wi01205557	Creating a new vlan port with a new mstp group does not forward any traffic on IST ports.	Work around by ensuring that the port is in down state before adding to the VLAN. Enabling port afterwards will clear the STG blocking state. Otherwise use existing STG.

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!!!

Refer to Quick Install guide (NN46250-102) for New Chassis Installation Best Practices.

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 © 2015 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>