Virtual Services Platform 9000 Software Release 3.4.2.1

1. Release Summary

Release Date: July 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.3.4.2.1.tgz	Release 3.4.2.1 archived software distribution	114737934
VSP9K.3.4.2.1_modules.tgz	Release 3.4.2.1 Encryption Modules	41894

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.3.4.2.1.tgz
software add-modules 3.4.2.1.GA VSP9K.3.4.2.1_modules.tgz
software activate 3.4.2.1.GA

6. Version of Previous Release

Software Version 3.4.0.2, 3.4.1.0, 3.4.2.0

7. Compatibility

8. Changes in 3.4.2.1

New Features in This Release

Old Features Removed From This Release

Removed "show snmplog file" option.

Problems Resolved in This Release

ID	Description
wi01171052	Traffic not reaching intended destination. Malformed ISIS CSNP packets may cause duplicate LSP entries and result in missing FIB entries.
wi01174742	Multiple Qualys scans may cause memory corruption and reset of CP.
wi01175849	Copying from the /usb drive using a wild card does not work.
wi01176055, wi01069654	Modified Qe2K exception detection and recovery logic to prevent VLACP and SMLT flap.
wi01176057, wi01151846	Fully populated VSP9K chassis may falsely signal IO/CP heartbeat issues on bootup.
wi01176374, wi01172237	Corrupted SNMPLOG file may cause reset of CP when display attempted using "show snmplog file" Remove deprecated snmplog file option since SNMPLOG entries are integrated in the unified log file.
wi01176855, wi01168516	9024XL continuously logging this error: IO4 [04/17/14 05:00:29.077] 0x001205ea 00000000 GlobalRouter COP-SW ERROR BCMSDK unit = 4, L3_ENTRY_ONLY, entry 3971 parity error.

wi01176970	OpenSSL CVE-2014-0224, Man-in-the-middle attack
wi01177352, wi01173652	Ping timeout seen even if destination is reachable

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 .

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