avaya.com

Virtual Services Platform 9000 Software Release 4.1.4.0

1. Release Summary

Release Date: March 2017
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 4.1.0.0 (NN46250-401) 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.4.1.4.0.tgz	Release 4.1.4.0 archived distribution	176792351
VSP9K.4.1.4.0_modules.tgz	Encryption modules	41905
VSP9K.4.1.4.0_mib.zip	Archive of all MIB files	825433

VSP9K.4.1.4.0_mib.txt	MIB file	10984592
VSP9K.4.1.4.0_mib_sup.txt	MIB file	957963
VSP9000v410_HELP_EDM_gzip.zip	EDM Help file	3882169
VSP9K.4.1.4.0.md5	MD5 Checksums	586
VSP9K.4.1.4.0.sha512	SHA encryption	1546
VSP9000v4.1.4.0.zip	EDM WAR plugin for COM	5656349

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.4.1.4.0.tgz
software add-modules 4.1.4.0.GA VSP9K.4.1.4.0_modules.tgz
software activate 4.1.4.0.GA

6. Version of Previous Release

Software Version 3.4.x.x, 4.0.0.0, 4.0.1.0, 4.0.1.1, 4.0.1.2, 4.1.0.0, 4.1.1.0, 4.1.2.0, 4.1.3.0

7. Compatibility

8. Changes in 4.1.4.0

New Features in This Release

None

Old Features Removed From This Release

None

Problems Resolved in This Release

Issue Number	Issue Description
VSP9000-708	On Gen-2 IO modules, continuous flapping of ISIS adjacencies in the system may result in the exhaustion of heap memory associated with SPB ARP table. This heap memory exhaustion may cause system instability and network connectivity issues.
VSP9000-712	MAC learning will be stopped on ports when FDB violation condition is hit i.e., the number of MAC addresses learnt on these ports exceed the configured threshold limit. For easier debugging, an enhancement has been made to dump all the FDB entries learnt on these ports into a file "/intflash/portFdbViolation.txt" during FDB violation.
VSP9000-716	In systems with Gen-2 IO modules, VRRP mastership contention may be seen due to incorrect propagation of VRRP control packets received over NNI links.
VSP9000-718	Duplicate Nickname connected to existing SPBM topology caused network outage. • SPBM ISIS Duplicate System Id/Nickname Detection. Enhancements were made to the SPBM code in all products to help prevent network outages caused by duplicate misconfigurations of Nickname and/or System-id. ○ The upgraded code has algorithms to detect duplicate system-id and/or Nickname when a node is introduced into the SPB network. When duplication is detected the newly added duplicate system is isolated from the SPBM network by automatically disabling ISIS and the existing SPBM nodes perform clean-up activities for the corruption introduced. ○ The recovery procedure is as follows depending on which entity was duplicated: a. If both the Nickname and System-id were duplicated, then both need to be made unique and ISIS re-enabled b. If only the System-id was duplicated then the Nickname needs to be changed, the System-id needs to be made unique and ISIS re-enabled c. If only the Nickname was duplicated, then: 1. Either wait 20 minutes for the LSPs from that System-id to age out of the network, make the Nickname unique and re-enable ISIS 2. Or if the node needs to be introduced into the network immediately, make the Nickname unique, change the System-id and re-enable ISIS

	○ A CLI consistency check was introduced to prevent a virtual BMAC being erroneously configured equal to the “system-id” or the “IST peer’s system-id”. ○ To help administrators identify and avoid introducing a duplicate, the existing CLI command “show isis spbm nick-name” was augmented to include all system identifications that need to be unique: LSP-id /system-id, Nickname, Virtual BMAC and Host name. ○ Filtering by nick-name, smlt-virtual-bmac and sysid options were added to the "show isis spbm nick-name" command. VSP-9000:1#show isis spbm nick-name ISIS SPBM NICK-NAME LSP ID LIFETIME NICK-NAME VIRTUAL-BMAC HOST-NAME 00bb.1000.8037.00-00 553 1.80.37 00:bb:10:80:37:ff VSP9012#2-10.139.80.35 00bb.1000.8047.00-00 302 1.80.47 00:bb:10:80:37:ff VSP9012#2-10.139.80.35 00bb.1000.8721.00-00 832 1.87.21 00:bb:87:21:00:ff VSP7024-87.21 00bb.1000.8722.00-00 825 1.87.22 00:bb:87:21:00:ff VSP7024-87.22 00bb.1000.8730.00-00 614 1.87.30 00:bb:87:30:00:ff BUS-DC-VSP8284-A-87.30 00bb.1000.8731.00-00 623 1.87.31 00:bb:87:30:00:ff BUS-DC-VSP8284-B-87.31 00bb.1000.8732.00-00 681 1.87.32 00:bb:87:32:00:ff Top-VSP4K-4850GTS-PWR+-87.32 00bb.1000.8733.00-00 742 1.87.33 00:bb:87:32:00:ff Bottom-VSP4K-4850GTS-87.33 00bb.1000.8736.00-00 906 1.87.36 00:bb:87:36:00:ff BCore-9000A 00bb.1000.8739.00-00 864 1.87.39 00:bb:87:36:00:ff CCore-9000A 00bb.1000.8744.00-00 372 1.87.44 00:bb:87:44:00:ff VSP-7254XSQ-87.44 00bb.1000.8745.00-00 393 1.87.45 00:bb:87:44:00:ff VSP-7254XSQ-87.45 00bb.1000.8751.00-00 560 1.87.51 00:00:00:00:00:00 ERS5928GTSPWR+87-51 00bb.1000.8752.00-00 544 1.87.52 00:00:00:00:00:00 VSP4450GTXHT-10.139.87.52 00bb.1000.8753.00-00 784 a.d0.01 00:bb:87:53:00:ff 8600-8753 00bb.1000.8755.00-00 811 a.d0.12 00:bb:87:53:00:ff 8600-8755
VSP9000-719	Stale static inter-VRF routes are observed in the system when the next-hop VRF is deleted. The stale route entries may result in system reset.
VSP9000-727	Running periodic scans on IPv6 module can cause system instability and system may reset due to memory corruption.

VSP9000-728	When PCAP capture-filter is enabled, egress IP packets are not captured even though they match the capture criteria.
VSP9000-739	When system is coming up after a reboot, there may be loss of IP shortcut traffic due to IP shortcut routes not honoring overload on startup timer.

10. Outstanding Issues

Please see "Virtual Services Platform 9000, Release Notes" for software release 4.1.0.0 (NN46250-401), 4.1.1.0, 4.1.2.0 and 4.1.3.0 available at http://www.avaya.com/support for details regarding Known Issues.

11. Known Limitations

Please see "Virtual Services Platform 9000, Release Notes" for software release 4.1.0.0 (NN46250-401), 4.1.1.0, 4.1.2.0 and 4.1.3.0 available at http://www.avaya.com/support for more details regarding Known Limitations.

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 .