VSP Operating System Software Release 5.1.1.5

1. Release Summary

Release Date: March 2017
Purpose: Software release to address customer found software issues.

2. Important Notes before Upgrading to This Release

If upgrading systems from either release 4.2.1.0 or release 4.2.1.1 that have ISIS enabled link(s) configured with HMAC-MD5 authentication then you need to perform the procedure described in section (4) below in order to avoid potential network connectivity loss.

If upgrading systems running 4.1.X releases which also have TACACS+ enabled refer to section 4 for upgrade instructions.

3. Platforms Supported

Virtual Services Platform 4000 Series
- Virtual Services Platform VSP 4850GTS
- Virtual Services Platform VSP 4850GTS-PWR+
- Virtual Services Platform VSP 4450GSX-PWR+
- Virtual Services Platform VSP 4450GSX-DC
- Virtual Services Platform VSP 4450GTS-DC
- Virtual Services Platform VSP 4450GTX-HT-PWR+

Virtual Services Platform 7200 Series
- Virtual Services Platform VSP 7254XSQ
- Virtual Services Platform VSP 7254XTQ

Virtual Services Platform 8000 Series
- Virtual Services Platform 8200
- Virtual Services Platform 8400

.

4. Special Instructions for Upgrade from previous releases

1. The following procedure should be followed when upgrading systems running one of the following two releases, 4.2.1.0 or 4.2.1.1 which also have ISIS enabled links with HMAC-MD5 authentication on:

   Disable ISIS authentication throughout the network a system at a time, a link at a time by disabling it on either side of each link, ensuring the link is stable before moving to the next. When a system has been reconfigured free of ISIS HMAC-MD5 authentication in all of its links, save the configuration file and perform the upgrade to release 4.2.3.0 or greater. After all these systems have been upgraded to release 4.2.3.0 or greater, you may re-enable authentication a system at a time, a link at a time and save the configuration file in each of the involved systems.

Example:

```
VSP:1(config)#interface gigabitethernet x/y
VSP:1(config-if)#no isis hello-auth
VSP:1(config-if)#save config
VSP:1(config-if)# PERFORM THE UPGRADE
VSP:1(config)#interface gigabitethernet x/y
VSP:1(config-if)# isis hello-auth type hmac-md5 key <keyname> [key-id <keyed>]
VSP:1(config-if)#save config
```

2. The following procedure should be followed when upgrading systems running 4.1.X releases which also have TACACS+ enabled on:

   When you upgrade from VOSS 4.1.X to VOSS 4.2 or a higher release, the TACACS+ host configurations will be lost. After the upgrade, the TACACS+ host configurations will not take effect so you must reconfigure them. After you make the configurations, you must save the changes on the device. You should also save the configuration to a file to retain the configuration settings.

5. Notes for Upgrade

Please see "Release Notes for VSP Operating System" for software release 5.1.1 (NN47227-401, 09.04) available at http://www.avaya.com/support for details on how to upgrade your Switch.

File Names For This Release

Virtual Services Platform 4000 Series

File Name	Module or File Type	File Size (bytes)
VOSS4K.5.1.1.5.tgz	Release 5.1.1.5 archived software distribution	97255354
VOSS4K.5.1.1.5_mib.zip	Archive of all MIB files	996418
VOSS4K.5.1.1.5_mib.txt	MIB file	6681002
VOSS4K.5.1.1.5_mib_sup.txt	MIB file	987668
VSP4000v511_HELP_EDM_gzip.zip	EDM Help file	2996205
VSP4000v5.1.1.4.zip	EDM plug-in for v5.1.1.4/vsp4000	4503221
VOSS4K.5.1.1.5.md5	MD5 Checksums	642

Virtual Services Platform 7200 Series

File Name	Module or File Type	File Size (bytes)
VOSS7K.5.1.1.5.tgz	Release 5.1.1.5 archived software distribution	62810362
VOSS7K.5.1.1.5_mib.zip	Archive of all MIB files	996418
VOSS7K.5.1.1.5_mib.txt	MIB file	6681002
VOSS7K.5.1.1.5_mib_sup.txt	MIB file	980646
VOSSv511_HELP_EDM_gzip.zip	EDM Help file	3017523
VOSSv5.1.1.4.zip	EDM plug-in for v5.1.1.4/vsp7200	4637184
VSP7K.5.1.1.5.md5	MD5 Checksums	636

Virtual Services Platform 8000 Series

File Name	Module or File Type	File Size (bytes)
VOSS8K.5.1.1.5.tgz	Release 5.1.1.5 archived software distribution	62817324
VOSS8K.5.1.1.5_mib.zip	Archive of all MIB files	996418
VOSS8K_5.1.1.5_mib.txt	MIB file	6681002
VOSS8K.5.1.1.5_mib_sup.txt	MIB file	980646
VOSSv511_HELP_EDM_gzip.zip	EDM Help file	3017523
VOSSv5.1.1.4.zip	EDM plug-in for v5.1.1.4/vsp8000	4637184
VSP8K.5.1.1.5.md5	MD5 Checksums	636

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 procedures:

```
software add VOSS4K.5.1.1.5.tgz
software activate VOSS4K.5.1.1.5.GA
```

or

```
software add VOSS7K.5.1.1.5.tgz
software activate VOSS7K.5.1.1.5.GA
```

or

```
software add VOSS8K.5.1.1.5.tgz
software activate VOSS8K.5.1.1.5.GA
```

6. Version of Previous Release

Virtual Services Platform 4000 Series

Software Version 3.0.0.0, 3.0.1.0, 3.1.0.0, 3.1.0.2, 3.1.0.3, 4.0.0.0, 4.0.0.1, 4.0.0.2, 4.0.0.3, 4.1.0.0, 4.1.0.1, 4.2.0.0, 4.2.0.1, 4.2.1.0, 4.2.1.1, 4.2.2.0, 4.2.3.0, 5.0.0.0, 5.0.1.0, 5.1.0.0, 5.1.1.0, 5.1.1.1, 5.1.1.2, 5.1.1.3 and 5.1.1.4 for VSP 4850GTS platforms

Software version 4.0.0.0, 4.0.0.1, 4.0.0.2, 4.0.0.3, 4.1.0.0, 4.1.0.1, 4.2.0.0, 4.2.0.1, 4.2.1.0, 4.2.1.1, 4.2.2.0, 4.2.3.0, 5.0.0.0, 5.0.1.0, 5.1.0.0, 5.1.1.0, 5.1.1.1, 5.1.1.2, 5.1.1.3 and 5.1.1.4 for VSP 4450GSX platform

Software Version 4.0.50.0 4.2.1.1, 4.2.2.0, 4.2.3.0, 5.0.0.0, 5.0.1.0, 5.1.0.0, 5.1.1.0, 5.1.1.1, 5.1.1.2, 5.1.1.3 and 5.1.1.4 for VSP 4450GSX DC and VSP 4450GTS DC platforms

Software Version 4.0.40.0**,** 4.1.0.0, 4.1.0.1, 4.2.0.0, 4.2.0.1, 4.2.1.0 4.2.1.1, 4.2.2.0, 4.2.3.0, 5.0.0.0, 5.0.1.0, 5.1.0.0, 5.1.1.0, 5.1.1.1, 5.1.1.2, 5.1.1.3 and 5.1.1.4 for VSP 4450GTX-HT-PWR+ platform

Virtual Services Platform 7200 Series

Software Version 4.2.1.0, 4.2.1.1, 4.2.2.0, 4.2.3.0, 5.0.0.0, 5.0.1.0, 5.1.0.0, 5.1.1.0, 5.1.1.1, 5.1.1.2, 5.1.1.3 and 5.1.1.4

Virtual Services Platform 8000 Series

Software Version 4.0.0.0, 4.0.1.0, 4.0.1.1, 4.0.1.2, 4.0.1.3, 4.0.1.4, 4.1.0.0, 4.1.0.1, 4.2.0.0, 4.2.0.1, 4.2.1.0, 4.2.1.1, 4.2.2.0, 4.2.3.0, 5.0.0.0, 5.0.1.0, 5.1.0.0, 5.1.1.0, 5.1.1.1, 5.1.1.2, 5.1.1.3 and 5.1.1.4 for VSP8200 platform

Software Version, 4.2.0.0, 4.2.0.1, 4.2.1.0, 4.2.1.1, 4.2.2.0, 4.2.3.0, 5.0.0.0, 5.0.1.0, 5.1.0.0, 5.1.1.0, 5.1.1.1, 5.1.1.2, 5.1.1.3 and 5.1.1.4 for VSP8400 platform

7. Compatibility

8. Changes in 5.1.1.5

New Features in This Release

Support for extended range SR4 40G module AA1404006 from Finissar

Old Features Removed From This Release

Problems Resolved in This Release

ID	Description
VOSS-3546 VOSS-4918	VSP8404 was unresponsive after reboot.
VOSS-4724	Inter-VRF static route where next-hop address is in another VRF was not being cleaned up properly when the nexthop is removed.
VOSS-5076	When using EDM, changing the VLAN configuration of a Tagged MLT composed of multiple vlans results in only the last VLAN being selected.
VOSS-5256	Add support for new extended range SR4 40G module AA1404006 from Finissar
VOSS-5274	CFM L2 ping/traceroute from a VOSS device towards an end device is failing when there are two ECMP paths on different SPBM vlans. Return path is selecting wrong interface.
VOSS-5413	LSDB detail sometimes incorrectly populating TLV 147 chassis mac with chassis mac associated with another nodes LDP information
VOSS-5602	Enhance SPB L3 Unicast to support overload bit for IP shortcut and IPv6 Routes.
VSP4000-129	Netboot process fails for Apple Mac PC when DHCP-relay is configured on VSP 4450 switches running SPBM-L2VSN
VSP4000-133	Inconsistency in EDM LED Status With Physical Device LED Status
VSP4000-134	ISIS logical adjacency does not re-establish when the physical port containing the IP tunnel is bounced. In this scenario, the ISIS control packets are sent with a source mac of all zeros, leading to any intermediate L2 devices between the logical adjacency endpoints dropping the packet.
VSP4000-135	Syslog showed passwords and SNMP community strings in the clear.
VSP4000-138	Trace level 125 is defaulted to very terse. This results in a large number of PLSB/ISIS related messages in the trace file.
VSP4000-144	VSP4000 datapath support of IP Directed Broadcast using port 1/46
VSP4000-141	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. o 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. o 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-8404-87-49:1#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
```

VSP4000-150	Changes to an OSPF interface metric via EDM are not reflected in the running config
VSP7200-14	L3VSN traffic destined for routes within a VRF context that learned any routes via ISIS

	accept policies may get dropped.
VSP8000-157	VRRP Hold-down timers do not come into effect at the same time for multiple VRRP instances during failover tests.
VSP8000-166	ARP table Entry maybe learned in wrong VRF context after disabling an NNI Link.
VSP8000-168	Switch may reset when deleting a VRF and a static route which has a next hop in the deleted VRF. Consistency check added to not allow VRF deletion until all routes that refer to the VRF are deleted.
VSP8000-171	VSP 8000 crash during a FTP upload

9. Outstanding Issues

Please see “Release Notes for VSP Operating System” for software release 5.1.1 (NN47227-401, 09.04) available at http://www.avaya.com/support for details regarding Known Issues.

In addition, the following issues have been identified:

ID	Problem Description	Workaround

10. Known Limitations

Please see “Release Notes for VSP Operating System” for software release 5.1.1 (NN47227-401, 09.04) available at http://www.avaya.com/support for details regarding Known Limitations.

The VSP8284XSQ platform may experience a watchdog timeout induced reset when a momentary power loss to the system occurs. In this situation the datapath has been reinitialized even though there is enough power left in the system for the Control Plane to generate a coredump. The reset is needed for the system to be fully functional again. Using a UPS is recommended to mitigate momentary power interruption.

Regular cleanup of unneeded files on USB drives is recommended to minimize possibility of USB corruption when a system is reset, shutdown or power is lost.

Firefox 38 introduced more stringent crypto cipher requirements. If using versions 38 or higher please set the Firefox user configuration to enable fallback to RC4. The use of RC4 cipher is not supported starting Firefox 50. Otherwise use older version of Firefox or other supported browsers.

11. 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