VSP Operating System Software Release 4.2.2.0

1. Release Summary

Release Date: December 2015
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.

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

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 4.2.2.0. After all these systems have been upgraded to release 4.2.2.0 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:

©2015 Avaya Inc. Revision 1.0

```
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
```

5. Notes for Upgrade

Please see “Release Notes for VSP Operating System” for software release 4.2.1 (NN47227-401, 06.03) 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.4.2.2.0.tgz	Release 4.2.2.0 archived software distribution	110880504
VOSS4K.4.2.2.0_mib.zip	Archive of all MIB files	923544
VOSS4K.4.2.2.0_mib.txt	MIB file	6072204
VOSS4K.4.2.2.0_mib_sup.txt	MIB file	895680
VSP4000v421_HELP_EDM_gzip.zip	EDM Help file	2870067
VSP4000v4.2.2.0.zip	EDM plug-in for v4.2.2.0/vsp4000	4274219
VOSS4K.4.2.2.0.md5	MD5 Checksums	533

Virtual Services Platform 7200 Series

File Name	Module or File Type	File Size (bytes)
VOSS7K.4.2.2.0.tgz	Release 4.2.2.0archived software distribution	60684384
VOSS7K.4.2.2.0_mib.zip	Archive of all MIB files	923544
VOSS7K.4.2.2.0_mib.txt	MIB file	6072204
VOSS7K.4.2.2.0_mib_sup.txt	MIB file	994270
VOSSv421_HELP_EDM_gzip.zip	EDM Help file	2956707
VOSSv4.2.2.0.zip	EDM plug-in for v4.2.2.0/vsp7200	4375335
VSP7K.4.2.2.0.md5	MD5 Checksums	527

Virtual Services Platform 8000 Series

File Name	Module or File Type	File Size (bytes)
VOSS8K.4.2.2.0.tgz	Release 4.2.2.0 archived software distribution	60685107
VOSS8K.4.2.2.0_mib.zip	Archive of all MIB files	923544
VOSS8K.4.2.2.0_mib.txt	MIB file	6072204

©2015 Avaya Inc. Revision 1.0

VOSS8K.4.2.2.0_mib_sup.txt	MIB file	994270
VOSSv421_HELP_EDM_gzip.zip	EDM Help file	2956707
VOSSv4.2.2.0.zip	EDM plug-in for v4.2.2.0/vsp8000	4375335
VSP8K.4.2.2.0.md5	MD5 Checksums	527

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.4.2.2.0.tgz
software activate VOSS4K.4.2.2.0.GA

or

software add VOSS7K.4.2.2.0.tgz
software activate VOSS7K.4.2.2.0.GA

or

software add VOSS8K.4.2.2.0.tgz
software activate VOSS8K.4.2.2.0.GA

©2015 Avaya Inc. Revision 1.0

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 and 4.2.1.1 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 and 4.2.1.1 for VSP 4450GSX platform

Software Version 4.0.50.0 and 4.2.1.1 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 and 4.2.1.1 for VSP 4450GTX-HT-PWR+ platform

Virtual Services Platform 7200 Series

Software Version 4.2.1.0 and 4.2.1.1

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 and 4.2.1.1 for VSP8200 platform

Software Version, 4.2.0.0, 4.2.0.1, 4.2.1.0 and 4.2.1.1 for VSP8400 platform

7. Compatibility

8. Changes in 4.2.2.0

New Features in This Release

Old Features Removed From This Release

Problems Resolved in This Release

ID	Description
VSP4000-40 wi01231976	EDM Doesn't display VRF VLAN data using IE8
VSP4000-43	COM polling for L2VSN results in premier license violation logs when license has expired.
VSP4000-44	VSP4000 platform is not negotiating Rx flow control.

©2015 Avaya Inc. Revision 1.0

VSP4000-47	For VSP4000 GTX HT platform, 1G SFP in 10G SFP+ port is not working
VSP4000-48	Upgrading a VOSS platform to 4.2.1.1 with ISIS-MD5 HMAC encryption configured, ISIS links failed to come up because of interface re-indexing after upgrade. NOTE: See special instructions for upgrade in section (4) above.
VSP4000-49	ECMP route is not installed correctly when a slot is reset on a VOSS platform.
VSP4000-50	New Multicast streams maybe unable to be received by receivers across the SPB cloud. Critical resource is leaked when a local multicast stream (a stream ingressing via a UNI port) is cleaned up (either due to age out or local port down) prior to any NNI receivers being present for the stream.
VSP8000-27 wi01231922	Unable to configure OOB management IP address using Firefox Version 32
VSP8000-29 VSP8000-31 VSP8000-48	Intermittent memory corruption causes device reset on platforms with VLACP enabled on ports.
VSP8000-33	Device may reset while explicitly clearing a MAC address which contains special characters such as “-“, “|”, or “.”. Expected format is 0x00:0x00:0x00:0x00:0x00:0x00:0x00.
VSP8000-34	No log message is being generated when USB device is inserted or removed
VSP8000-36 VSP8000-42	Device stops forwarding traffic towards the default route. The error state can be resolved by deleting and re-adding the default route however the error state would return after an undetermined period of time. IO1 [10/08/15 09:34:29.025:EDT] 0x0014051a 00000000 GlobalRouter COP-SW ERROR ercdAddEcmpDefaultRoute: The new Number of ECMP Default Routes is not one greater than the existing routes. Current: 1, DpmMsg: 1 IO1 [10/08/15 09:34:29.025:EDT] 0x00140504 00000000 GlobalRouter COP-SW ERROR ercdProcArpRecMsg: Failed to Add ECMP Default Route This condition occurs when ECMP is enabled, and default route flaps due to ARP aging or any other reason.
VSP8000-37	Device resets due to Watchdog timer expiration while show fulltech is run in privilege mode
VSP8000-38	Packets with destination mac equal to the VRRP mac address were not being processed (routed) correctly, as the mac address was being incorrectly associated with a SMLT port before VRRP was enabled locally.
VSP8000-40	TTL of ARP for the next hop of a static route continues to decrement to 1 and then refreshes

	to 6.
VSP8000-41	The source IP address of the IGMP Group Specific Query is not always the same as the source IP address of the IGMP General Query. This inconsistency occurs when an IP address is assigned to the VLAN, and the "snoop-querier-address" parameter is not configured as part of IGMP.
VSP8000-43	When same source S and destination G exist for both sender and receiver, IGMP control message - group report is being forwarded out to the whole vlan instead of sending directly to CP, this causes the other ports in the vlan to stop replying to the query since it detects that another one has already replied.
VSP8000-44	Device resets while performing changes in IPv6 via EDM.
VSP8000-49 VSP8000-50	Device may reset when VLACP is enabled on ports.
VSP8000-52 wi01233932	Device resets while TACACS is enabled and Nessus scan is being run against that device.
VSP8000-54 wi01154718	VLACP Down PDUs are not being sent correctly in one way traffic case.
wi01228546	L1 configurations not always applied consistently at boot. boot combo ports 47 & 48 in back to back configuration at fixed speed 100 will come up at 1000 full.
wi01230401	TACACS configuration not showing correctly in Enterprise Device Manager

©2015 Avaya Inc. Revision 1.0

9. Outstanding Issues

Please see “Release Notes for VSP Operating System” for software release 4.2.1 (NN47227-401, 06.03) available at http://www.avaya.com/support for details regarding Known Issues.

In addition, the following issues have been identified:

ID	Problem Description	Workaround
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.
wi01222120	On VSP 8000 Series platforms IPv4 Filters with redirect next hop action is not forwarding when a default route is not present or a VLAN common to ingress VLAN of the filtered packet is not present.	Configure a default route if possible.

10. Known Limitations

Please see “Release Notes for VSP Operating System” for software release 4.2.1 (NN47227-401, 06.03) 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.

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 .

©2015 Avaya Inc. Revision 1.0

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