VSP Operating System Software Release 5.1.1.1

1. Release Summary

Release Date: June 2016
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 4.2.3.0 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
```

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.5.1.1.1.tgz	Release 5.1.1.1 archived software distribution	97213032
VOSS4K.5.1.1.1_mib.zip	Archive of all MIB files	995989
VOSS4K.5.1.1.1_mib.txt	MIB file	6679204
VOSS4K.5.1.1.1_mib_sup.txt	MIB file	986179
VSP4000v511_HELP_EDM_gzip.zip	EDM Help file	2886205
VSP4000v5.1.1.0.zip	EDM plug-in for v5.1.1.0/vsp4000	4500048
VOSS4K.5.1.1.1.md5	MD5 Checksums	533

Virtual Services Platform 7200 Series

File Name	Module or File Type	File Size (bytes)
VOSS7K.5.1.1.1.tgz	Release 5.1.1.1 archived software distribution	62783688
VOSS7K.5.1.1.1_mib.zip	Archive of all MIB files	995989
VOSS7K.5.1.1.1_mib.txt	MIB file	6679204
VOSS7K.5.1.1.1_mib_sup.txt	MIB file	979271
VOSSv511_HELP_EDM_gzip.zip	EDM Help file	3017523
VOSSv5.1.1.0.zip	EDM plug-in for v5.1.1.0/vsp7200	4631667
VSP7K.5.1.1.1.md5	MD5 Checksums	527

Virtual Services Platform 8000 Series

File Name	Module or File Type	File Size (bytes)
VOSS8K.5.1.1.1.tgz	Release 5.1.1.1 archived software distribution	62785018
VOSS8K.5.1.1.1_mib.zip	Archive of all MIB files	995989
VOSS8K_5.1.1.1_mib.txt	MIB file	6679204
VOSS8K.5.1.1.1_mib_sup.txt	MIB file	979271
VOSSv511_HELP_EDM_gzip.zip	EDM Help file	3017523
VOSSv5.1.1.0.zip	EDM plug-in for v5.1.1.0/vsp8000	4631667
VSP8K.5.1.1.1.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.5.1.1.1.tgz
software activate VOSS4K.5.1.1.1.GA
```

or

```
software add VOSS7K.5.1.1.1.tgz
software activate VOSS7K.5.1.1.1.GA
```

or

```
software add VOSS8K.5.1.1.1.tgz
software activate VOSS8K.5.1.1.1.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, and 5.1.1.0 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, and 5.1.1.0 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, and 5.1.1.0 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, and 5.1.1.0 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, and 5.1.1.0

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, and 5.1.1.0 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, and 5.1.1.0 for VSP8400 platform

7. Compatibility

8. Changes in 5.1.1.1

New Features in This Release

A new boot-flag named “minimum-ssl-version” has been introduced to allow user specified minimum SSL version supported on the switch, i.e, SSL2, SSL3 or TLS1. Default value is SSL3

Old Features Removed From This Release

Problems Resolved in This Release

ID	Description
VOSS-2629	Incorrect clean-up of internal SPBm records can cause connectivity issues over fabric

VSP4000-109	CLI allows configuration of half-duplex mode for copper ports which are unsupported on VSP8000. The VSP8400 will no longer allow the user to configure half-duplex on its port interfaces.
VOSS-2580	The VSP 7254 may not bring up link when using crossover cables The VSP7254 now operates properly with crossover cables.
VOSS-2618	SNMP agent address is seen to be 127.x.y.z address instead of configured CLIP when sending out trap on NNI interface
VSP8000-110	SSH login fails due to incorrect clean-up of SSH sessions leading to stale sessions when handling multiple SSH login/logout events at the same time.
VSP8000-103	Downstream directed broadcast packets go to CP causing high utilization and latency issues
VSP4000-94	EDM login failure due to SSL certificates that have the same serial number when logging in to multiple devices within a short span of time
VSP8000-102	VSP 8000 in-band management traffic (Telnet/SSH) not prioritized over other IP traffic leading to slowness and latency in managing the devices
VSP4000-102	LLDP enable or disable on the port/trunk level using MIB/EDM/CLI is not supported in this release.
VSP4000-105	VSP4850GTS does not support a trap to indicate disconnect of USB Added the trap and notification MIBs static OIDC_T RcnSystemUsbInternalAccessErrorTrapOid[] = {1,3,6,1,4,1,2272,1,21,0,335};
VSP4000-99	VSP4000GSX ports may not have consistent behavior when connected to devices without auto negotiation The VSP4000 will now implement "parallel detection" on all gigabit ports which enables links to be established in the case of mismatched layer 1 auto-negotiation settings.
VSP7200-4	Telnet packets leak from VRF to GlobalRouter without inter-VRF routing enabled
VOSS-2560	The following error message is printed for non-error condition. IO1 [04/25/16 16:15:57.080:EDT] 0x00140591 00000000 GlobalRouter COP-SW ERROR ercdSetDefaultRoute: Failed to add IPv4 Route in BCM for 0.0.0.0 mask=0.0.0.0 vrf=0: reason=0(Ok) Only print for failure case.
VOSS-2789	Stale static routes and incorrect ARP entries for the VRRP IP may be seen when VRRP is transitioned from Master to Back-up
VSP8000-114	NVD bulletin issues CVE-2016-0800, CVE-2005-0800 and CVE-2009-3555 have been addressed in this release. A new boot-flag named “minimum-ssl-version” has been introduced to allow user specified minimum SSL version supported on the switch, i.e, SSL2, SSL3 or TLS1. Default value is SSL3.“

VSP8000-122	VSP8000 SPB multicast traffic loss when directed broadcast enabled for the same VLAN

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.

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.

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