avaya.com

Virtual Services Platform 9000
Software Release 3.0.2.0

1. Release Summary

Release Date: March 18, 2011
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)

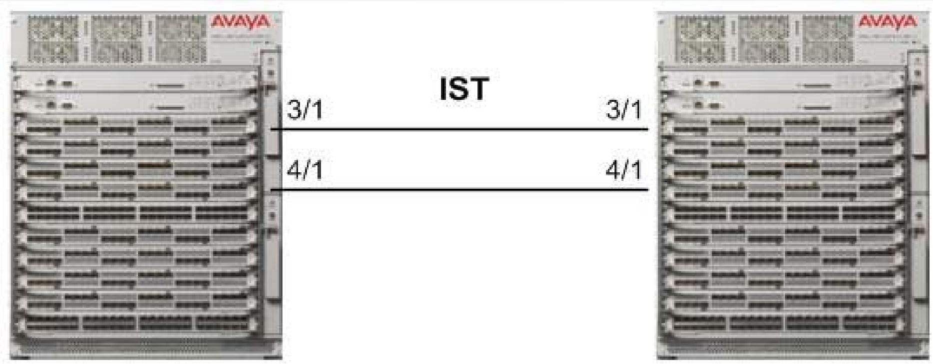
.

4. Special Instructions for Upgrade from 3.0.0.0

Special Upgrade Procedures for VSP Release 3.0.2.0

A recent [fix | change] applied to releases 3.0.1.0 and 3.0.2.0 (WI00859221) will prevent the IST protocol from establishing a connection to an IST peer VSP running release 3.0.0.0. To minimize network downtime when upgrading a pair of VSP core switches connected by an IST, the following procedure has been developed.

©2011 Avaya Inc. Revision 1.0



Step 1) Log into the console ports for each VSP and save your running configuration to ensure that it is correctly retrieved after the systems are reset.
Step 2) Transfer new software and modules .tgz files to each VSP. Then Add and Activate the new Software Release 3.0.2.0 on both nodes of the cluster.

software add VSP9K.3.0.2.0.tgz
software add-modules 3.0.2.0.GA VSP9K.3.0.2.0_modules.tgz
software activate 3.0.2.0.GA

Step 3) Orderly shutdown of non IST ports followed by IST ports in first VSP chassis to be upgraded.

a) Shutdown all of the non IST ports on the first VSP that is being upgraded.
This example assumes there are several ports on various line cards across various slots in the chassis. This example also illustrates how ports 3/1 and 4/1(the IST ports) can be excluded from the shutdown command that includes all of the non IST interfaces.

enable
config terminal
interface gigabitEthernet 3/2-3/48,4/2-12/48
shutdown
exit

The above commands will disable all of the non IST ports on the respective I/O Cards. Any traffic that was traversing this VSP via SMLT links will be switched to the other VSP in the SMLT based cluster through this step.

b) Shutdown all of the IST ports on the first VSP that is being upgraded.
This example again assumes that our IST ports on the first VSP that is being upgraded are 3/1 and 4/1.

interface gigabitEthernet 3/1,4/1
shutdown
exit

©2011 Avaya Inc. Revision 1.0

At this point all ports have been disabled on first VSP. Verify that all SMLT traffic is flowing correctly through the other node of cluster.
Do NOT save the configuration file on first VSP with the above ports shutdown.

Step 4) Reset the first VSP with command **reset -y**
The switch will reset and boot up with the newly activated code in approximately 3-4 minutes.

Step 5) Once the first VSP system comes up, login as the operator and commit the software upgrade on VSP by typing:

enable
software commit

At this point the first VSP will be running the new software version of code. The SMLT ports on this node will initially be locked physically link down while the IST channel attempts to establish to the peer node. The IST will not be established due to the mismatched IST control channel. After 60 seconds the SMLT ports on this node will be unlocked and allowed to physically link up.

Step 6) Orderly shutdown of non IST ports followed by IST ports in second VSP chassis to be upgraded.
a) Shutdown all of the non IST ports on the second VSP that is being upgraded.
This example assumes there are several ports on various line cards across various slots in the chassis. This example also illustrates how ports 3/1 and 4/1(the IST ports) can be excluded from the shutdown command that includes all of the non IST interfaces.

enable
config terminal
interface gigabitEthernet 3/2-3/48,4/2-12/48
shutdown
exit

The above commands will disable all of the non IST ports on the respective I/O Cards. Any traffic that was traversing this VSP via SMLT links will be switched to the other VSP in the SMLT based cluster through this step.

b) Shutdown all of the IST ports on the second VSP that is being upgraded.
This example again assumes that our IST ports on the second VSP that is being upgraded are 3/1 and 4/1.

interface gigabitEthernet 3/1,4/1
shutdown
exit

©2011 Avaya Inc. Revision 1.0

At this point all ports have been disabled on second VSP. Verify that all SMLT traffic is flowing correctly through the other node of cluster.
Do NOT save the configuration file on second VSP with the above ports shutdown.

Step 7) Reset the second VSP with command **reset -y**
The switch will reset and boot up with the newly activated code in approximately 3-4 minutes.

Step 8) Once the second VSP comes up, login in as the operator and commit the software upgrade on VSP by typing:

enable
software commit

After the reboot of the second VSP both nodes will now be running the same version of software and IST channel code, thus the IST channel will re-establish and SMLTs will return to working state.

Step 9) Verify that the IST and SMLTs have returned to regular operational status by typing:

show ist mlt - IST state for the IST channel should show UP
show mlt – This command can be used to validate current state of the IST as well as active SMLTs

5. Notes for Upgrade

Please see "*Virtual Services Platform 9000, Release Notes*" for software release 3.0.0 (NN46250-401, 01.03) 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.3.0.2.0.tgz	Release 3.0.2.0 archived software distribution	97705085
VSP9K.3.0.2.0_modules.tgz	Release 3.0.2.0 Encryption Modules	33491

6. Version of Previous Release

Software Version 3.0.1.0

7. Compatibility

8. Changes in 3.0.2.0

New Features in This Release

Added support for two dedicated mac addresses as mac DA for IST packets

Old Features Removed From This Release

None.

Problems Resolved in This Release

New cli commands were added to assist the operator in backing up the contents of intflash and extflash to a USB device. **(wi00870784, Wi00871924)**

A new cli command was added to display the compact flash device firmware version number. **(wi00870789)**

Under rare conditions of frequent IST link bouncing, an IST peer connection can get stuck in an initialization state. When this occurs the connection will not come up until a read timeout of 10 minutes expires. **(Wi00869769)**

Under rare conditions, the IST peer connection can experience an internal queuing fault which causes the connection to become a one-way communication path. When this occurs, the IST between the two systems becomes inoperative. A CP switchover or a system reset is required to correct the problem**. (wi00869369)**

The VSP is not correctly forwarding broadcast packets in some VRRP configuration scenarios. This causes interoperability issues when running with an 8600 in an SMLT triangle topology. **(wi00869365)**

EDM certificate authentication issues have been seen when HTTPS and the Firefox browser are used. **(wi00869829)**

Enabling PCAP and L2 Mirroring on the same port will cause the IO module to become unresponsive. When this occurs, an IO module reset is required. **(wi00865238)**

9. Changes in 3.0.1.0

New Features in This Release

Added support for two dedicated mac addresses as mac DA for IST packets

Old Features Removed From This Release

None.

Problems Resolved in This Release

ARP entries on standby may not be installed if a MAC is modified from previous entry. (**wi00857533**)

The SMLT IST auto logger has been enhanced to log warning messages more frequently when delays are experienced during the IST link establishment phase. The IST auto logger provides detailed information in the form of warning messages written to the log that specifically point out the reason for delays in bringing the IST link up. These messages appear in 15-second intervals for the first two minutes and every minute thereafter until the IST link comes up. **(wi00857521)**

The SMLT IST auto logger has been enhanced to include additional detailed log messages in the area of ARP. (**wi00857524**)

If the CP receives a packet that is destine for a black hole route with a TTL=1, the CP will respond with an ICMP response to the source of the packet with a TTL expiration message. This activity will fail when the source IP address is a black hole route. The lookup failure will cause the CP to crash and the standby CP to take over. **(wi00857839)**

Multicast packets with a source IP address of 0.0.0.0 on a multicast enabled VLAN can cause various error messages and potentially cause the data path to stop processing packets. The only way to correct this problem is to reset the IO card. **(wi00858053)**

X11 packets are not correctly classified when they traverse the VSP over an IST link. This classification error will cause X11 traffic to be dropped. **(wi00895221)**

DHCP Relay administered IP addresses are not correctly synchronized with the standby CP. This can cause routing problems after a CP switchover for DHCP acquired IP addresses. Clearing the ARP entries for the DHCP administered IP addresses after a CP switchover will clear the problem. **(wi00860313)**

Establishing an encrypted https management connection to the VSP using a Konqueror 4.4.5 Browser can cause the master CP to crash under certain conditions. The CP does not correctly handle encryption from this browser. **(wi00862056)**

The default route’s next hop is not properly synchronized to the standby CP. This can cause a routing problem if a second switchover occurs before the ARP entry for the default route’s next hop is refreshed. The operator can manually flush the ARP entry for the default route immediately after a switchover to avoid this problem. **(wi00863792)**

10. Outstanding Issues

None.

11. Known Limitations

Please see "*Virtual Services Platform 9000, Release Notes* release 3.0.0" (NN46250-401, 01.03) available at http://www.avaya.com/support for 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 .

Copyright © 2011 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.