Applying Upgrades and Patches to Avaya Virtual Services Platform 9000

Release 4.0
NN46250-400
Issue 06.01
December 2014

© 2014 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can

result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction 6
Purpose 6
Related resources 6
Documentation 6
Training 6
Viewing Avaya Mentor videos 6
Support 7
Searching a documentation collection 7
Chapter 2: New in this release 9
Features 9
Other changes 9
Chapter 3: Upgrade, patching, and encryption fundamentals 10
Image naming conventions 10
Consistent image management design 11
Image upgrade fundamentals 11
Patching fundamentals 12
Commit fundamentals 13
Commit 13
Encryption modules fundamentals 14
Interfaces 15
File storage options 15
Boot and configuration file sources 16
Behavior during boot cycle and redundant configuration files 16
New software files 17
Checksums 18
Downgrade considerations 18
Chapter 4: Administrative procedures 19
Downloading the software 19
Backing up configuration files 20
Backing up and restoring the compact flash to USB 20
Configuring auto-commit 22
Disabling auto-commit 23
Copying files 24
Determining available storage space 25
Enabling FTP and TFTP 26
Specifying configuration file sources 26
Chapter 5: Software upgrade 28
Upgrading the software 28
Verifying the upgrade 34

Committing an upgrade 34
Downgrading the software 35
Performing a VSP 9000 network hitless upgrade 36
Chapter 6: Software patch 40
Patching the software 41
Verifying the patch 43
Committing a patch 43
Removing a patch 44
Aborting a patch 45
Chapter 7: Encryption module installation 47
Adding an encryption module 47
Chapter 8: Translations of safety messages 49
Class A electromagnetic interference warning statement 49
Electrostatic discharge caution statement 50
Glossary 52

Chapter 1: Introduction

Purpose

This document provides useful information to upgrade the software image, install patches, and add encryption modules to the Avaya Virtual Service Platform 9000.

For information about how to install or transfer licenses, see *Administering Avaya Virtual Services Platform 9000,* NN46250-600.

Related resources

Documentation

See *Documentation Reference for Avaya Virtual Services Platform 9000,* NN46250-100 for a list of the documentation for this product.

Training

Ongoing product training is available. For more information or to register, you can access the website at http://avaya-learning.com/.

Course code	Course title
4D00010E	Knowledge Access: ACIS - Avaya ERS 8000 and VSP 9000 Implementation
5D00040E	Knowledge Access: ACSS - Avaya VSP 9000 Support

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Searching a documentation collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.

2. Navigate to the folder that contains the extracted files and open the file named <*product_name_release*>.pdx.
3. In the Search dialog box, select the option **In the index named <*product_name_release*>.pdx**.
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
   - Whole Words Only
   - Case-Sensitive
   - Include Bookmarks
   - Include Comments
6. Click **Search**.

   The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance Ranking.

Chapter 2: New in this release

The following sections detail what is new in *Applying Upgrades and Patches to Avaya Virtual Services Platform 9000,* NN46250-400 for Release 4.0.

Features

There are no feature-related changes for Release 4.0.

Other changes

See the following sections for information about changes that are not feature-related.

Document title change

In Release 4.0, the title of this document changed from *Avaya Virtual Services Platform 9000 Upgrades and Patches*, NN46250-400 to *Applying Upgrades and Patches to Avaya Virtual Services Platform 9000,* NN46250-400.

Downloading the software

Release 4.0 changes the location of software downloads. For more information, see Downloading the software on page 19.

Chapter 3: Upgrade, patching, and encryption fundamentals

This chapter covers useful information for upgrading the software image, installing patches and adding encryption modules to the Avaya Virtual Service Platform 9000. Review the concepts in this section before performing all upgrade, patch, or add module procedures.

For the complete list and sizes of files that you require to upgrade, patch, or add modules, and last-minute procedure changes, see the Release Notes or ReadMe files which accompany the software release. You can download these documents from the Avaya Technical Support website: www.avaya.com/support.

Image naming conventions

VSP 9000 software and patch images use a standardized dot notation format. This standardized format is as follows:

- **Software images**

  Software images use the following format:

  Product Name.Major Release.Minor Release.Maintenance Release.Maintenance Release Update.tgz

  For example, the image file name **VSP9K.3.0.0.0.tgz** denotes a software image for the VSP9K product with a major release version of 3, a minor release version of 0, a maintenance release version of 0 and a maintenance release update version of 0. **TGZ** is the file extension.

  The image file name **VSP9K.3.1.0.0.tgz** denotes a software image for the VSP9K product with a major release version of 3, a minor release version of 1, a maintenance release version of 0 and a maintenance release update version of 0. **TGZ** is the file extension.

- **Software patch images**

  Software patch images follow a similar naming format to software images. The only difference is the addition of a patch ID at the end of the of the file name. The patch ID begins with a **T** to indicate hitless patches and a **R** to indicate reset patches.

  To illustrate the naming convention, consider the following example filename: **VSP9K.3.0.0.0–T02099198A.tgz** This filename indicates a hitless software patch that applies to Release 3.0.0.0. The patch ID is T02099198A.

Consistent image management design

The software upgrade and patching features have been designed for consistent behavior and functionality. The ACLI provides commands that affect some features simultaneously and other commands that only affect a single feature at a time. The following chart provides a high level view of this consistent behavior. Image management, image upgrades, and image patching provide a consistent, four step process regardless of the action to be taken.

Hitless patching	Reset patching	Image upgrades
1. Transfer patch to internal flash or other storage medium. 2. **`software patch add WORD<1-255>`** Unzips patch file and places it on the internal flash. 3. **`software patch apply patch-ids WORD<1-255>`** Applies the patch. 4. **`software patch commit`** Commits the software patch application request started in step 3. Auto-commit will be triggered if it is enabled and this command is not executed.	1. Transfer patch to internal flash or other storage medium. 2. **`software patch add WORD<1-255>`** Unzips patch file and places it on the internal flash. 3. **`software patch apply patch-ids WORD<1-255>`** Applies the patch. 4. **`software patch commit`** Commits the software patch application request started in step 3. Auto-commit will be triggered if it is enabled and this command is not executed.	1. Transfer image to internal flash or other storage medium. 2. **`software add WORD<1-99>`** Unzips image file and places it on the internal flash. 3. **`software activate WORD<1-99>`** Installs the image into the boot flash. 4. **`software commit`** Commits the new running image to Gold status. Auto-commit will be triggered if it is enabled and this command is not executed.

The software or patch image comes in the form of a TGZ zipped file. You do not need to unzip these files as the **`software add`** or **`software patch add`** commands handle the unzip. After you add and activate a software image, you must restart the system to run the new image. For more information about the **`software commit`** and **`software patch commit`** commands, see Software Commit (upgrade) on page 13 and Software Patch Commit on page 14.

Image upgrade fundamentals

This section details what you must know to upgrade the Virtual Services Platform 9000.

Upgrades

Install new software upgrades to add functionality to the Virtual Services Platform 9000. Major and minor upgrades are released depending on how many features the upgrade adds or modifies.

Upgrade time requirements

Image upgrades take less than 30 minutes to complete. The Virtual Services Platform 9000 continues to operate during the image download process. A service interruption occurs during the

installation and subsequent reset of the device. The system returns to an operational state after a successful installation of the new software and device reset.

Upgrade considerations

The Virtual Services Platform 9000 does not support different software versions running at the same time. For example, Release 3.2 on the primary Central Processor (CP) module and Release 3.0 on the secondary CP module.

Before you upgrade the software image

Before you upgrade the Virtual Services Platform 9000, ensure that you read the entire upgrading procedures.

You must keep a copy of the previous configuration file (config.cfg), in case you need to return to the previous version. The upgrade process automatically converts, but does not save, the existing configuration file to a format that is compatible with the new software release. The new configuration file may not be backward compatible.

Patching fundamentals

A patch is a small piece of software designed to fix and correct a problem in software code, its supporting data, or update a feature. The VSP 9000 platform software is the first ADS product to implement true patching. Avaya uses patching to deliver bug fixes and feature enhancements in a faster and simpler fashion than a full software upgrade. Avaya also uses patching to deliver debug code to gather debugging information at customer sites. Virtual Services Platform 9000 supports two types of patching:

- hitless patch

  The essence of hitless patching is that the target software is patched without disruption to running system processes. As a general rule, hitless patches will be the primary mode of patch creation. Other patching options will be considered only if all options to create a hitless patch have been exhausted.

- reset patch

  Reset patches are provided as an alternative form of patching when a hitless patch cannot be created as a fix for a problem. After you apply reset patches to the target software, you must reset the system for the patches to take effect. There will be a service outage and disruption of traffic when the system is reset.

Before you apply a patch to a running system, ensure that you read the readme file that came with the patch as well as this patching document. Download patches and readme files from the Avaya Support websit: www.avaya.com/support.

The following table lists patch states as they are applied or reverted.

Table 1: Patch states

State	Description
Available (av)	After you add the file using the **software patch add** command if the patch does not match the current software version.
Candidate (ca)	After you add the file using the **software patch add** command if the patch matches the current software version.
Applied (ap)	After you activate the patch using the **software patch apply** command.

Commit fundamentals

This section contains information about the commit function for the VSP 9000.

Note:

Gold status is software that has been committed. You can commit the software to gold by manually issuing the **software commit** command or automatically by enabling the auto-commit option.

Commit

The commit function of the Virtual Services Platform 9000 protects the system in case of an upgrade or patch failure. The VSP 9000 software incorporates a unified approach to committing software changes. The underlying architecture for software updates is shared between upgrades and patches. This includes the commit timer, software reset-commit-time, auto-commit functionality, and enabling of software changes. Use the **software commit** command when committing software upgrades and the **software patch commit** command for committing software patches as there are syntactical differences between the two commands.

Software commit (upgrade)

The software commit command for software upgrades allows maximum time set by the commit timer (the default is 10 minutes) to ensure a successful upgrade. If you enable the auto-commit option, the system automatically commits to the new software version after the commit timer expires. If you disable the auto-commit option, you must issue the software commit command before the commit timer expires to commit the new software version, otherwise the system restarts automatically to the previous (committed) version. To extend the time to commit the software after an upgrade, you can use the **software reset-commit-time** command. You can extend the time between 1 and 60 minutes.

Software patch commit

The **software patch commit** command for software patches allows maximum time set by the commit timer (the default 10 minutes) to ensure success of the applied patch. To extend the time to commit the software after applying a patch, you can use the **software reset-commit-time** command. You can extend the time between 1 and 60 minutes.

Hitless Patch

Apply a hitless patch:

- If the auto-commit option is enabled: the system automatically commits the hitless patch after the commit timer expires.
- If the auto-commit option is not enabled: you must issue the **software patch commit** command before the commit timer expires to commit the hitless patch, otherwise the system automatically reverts the hitless patch.

Reset Patch

Apply a reset patch and reset the system for the patch to take-effect:

- If the auto-commit option is enabled: the system automatically commits the reset patch after the commit timer expires.
- If the auto-commit option is not enabled: you must issue the **software patch commit** command before the commit timer expires to commit the reset patch, otherwise the system automatically restarts to revert the reset patch

.

Encryption modules fundamentals

This section details what you must know to add encryption modules to the Virtual Services Platform 9000.

Encryption modules

You can add encryption modules to the Virtual Services Platform 9000 to encrypt secure information, such as passwords, before the system sends the information to another device on the network. You must download and install the encryption modules for your software release, which are available in a separate archive.

You can add the following encryption modules to a Virtual Services Platform 9000 software release:

- Triple Data Encryption Standard (3DES)
- Advanced Encryption Standard (AES), which also includes Secure Shell encryption

Before you add an encryption module to the Virtual Services Platform 9000 software, ensure that you read the entire procedure.

Interfaces

You can apply patches and upgrades, and add encryption modules to the Virtual Services Platform 9000 using the Avaya Command Line Interface (ACLI).

For more information about ACLI, see *Using ACLI and EDM on Avaya Virtual Services Platform 9000,* NN46250-103.

File storage options

This section details what you must know about the internal boot and system flash memory, Universal Serial Bus (USB) mass-storage device, and external flash, which you can use to store the files that start and operate the Virtual Services Platform 9000.

The Virtual Services Platform 9000 file system uses long file names.

Internal flash

The Virtual Services Platform 9000 has two internal flash memory devices: the boot flash memory and the system flash memory. The system flash memory size is 2 gigabytes (GB).

Boot flash memory is split into two banks that each contain a different copy of the boot image files. Only the Image Management feature can make changes to the boot flash.

The system flash memory stores configuration files, runtime images, the system log, and other files. You can access files on the internal flash through the /intflash/ folder. Storage of the system log on the internal flash memory raises an alarm because the external flash is the preferred location. Ensure that external compact flash memory is properly installed so that the system log is stored there.

External flash and USB device

The VSP 9000 uses an external compact flash card and USB device for additional storage of configuration files, release images, and other files. The USB device provides a convenient, removable mechanism for moving files between VSP 9000 systems. In cases where network connectivity has not yet been established or network file transfer is not feasible, you can use the USB device to update the configuration and image files on a number of VSP 9000 systems.

Access files stored on the external flash through the /extflash/ folder. Access files stored on the USB device through the /usb/ folder.

Avaya recommends that you use a USB device or FTP server for file transfer.

File Transfer Protocol

You can use File Transfer Protocol (FTP) to load the software directly to the Virtual Services Platform 9000, or to download the software to the internal flash memory, external flash, or USB device.

The Virtual Services Platform 9000 can act as an FTP server. If you enable the FTP daemon (ftpd), you can use a standards-based FTP client to connect to the Control Processor (CP) module by

using the ACLI log on parameters. Copy the files from the client to either the internal flash memory or external flash.

Storage option considerations

Each storage choice has advantages and disadvantages. Consider the following when you make a storage decision:

- Internal compact flash is best suited for the storage of software and patch images, core files, and configuration files.
- External compact flash is best suited for the storage of log files.
- USB devices are best suited for moving files between VSP 9000s although ultimately FTP is the best solution for file transfer. USB devices provide the convenience of downloading software to one device to update many chassis, especially in instances where network connectivity precludes the use of an FTP server.

The upgrade procedures in this document assume that you copy the new software from a FTP server to the internal flash memory. However, you can use other storage options if you use the correct file names and paths during the procedures.

Boot and configuration file sources

The Virtual Services Platform 9000 stores the software images on the internal boot flash by default. You can use the **`boot config choice`** command to configure the system to load the configuration file from either the internal flash memory, the external flash, or a USB device.

The config.cfg file, which is the default configuration file, stores the configuration options of the Virtual Services Platform 9000 and of all the modules. You can use the **`boot config choice`** command to assign primary configuration and backup locations of the configuration files on your system. You can put the configuration files on the internal flash, external flash, or USB device.

For more information about boot sources, see *Administering Avaya Virtual Services Platform 9000,* NN46250-600.

Behavior during boot cycle and redundant configuration files

Avaya recommends that you take special care when you provide the boot options for the Virtual Services Platform 9000. You can configure a primary configuration file, as well as a backup configuration file.

In normal operation, Avaya recommends that you save the primary configuration file on the internal flash, and that you store the primary backup configuration file on the external compact flash to ensure that the Virtual Services Platform 9000 can start from an alternative file or drive in case the primary file or drive is unavailable. After you make changes to the configuration files, Avaya further

recommends that you save the last known good configuration as the backup configuration file. For more information about how to configure primary and backup configuration files, see Specifying configuration file sources on page 26.

Caution:

Risk of network outage

If the Avaya Virtual Services Platform 9000 cannot access a valid configuration file, it loads a default configuration, which can cause a network outage.

Ensure a valid configuration file is always available.

The following table shows how the Virtual Services Platform 9000 behaves in different boot situations. The system action column describes the expected behavior.

Table 2: System behavior during boot cycle

Parameters	System action
A configuration file is not specified. The config.cfg file is present on the flash drive.	The Virtual Services Platform 9000 starts using config.cfg.
The primary configuration file is specified. The configuration file is present on the flash drive.	The Virtual Services Platform 9000 starts using the specified configuration file.
The primary configuration file is specified. The configuration file is not present on the flash drive.	The Virtual Services Platform 9000 starts using factory defaults (if `boot config flags verify-config` is **`true`**, and a backup configuration is not specified).
The primary configuration file is specified. The configuration file on the flash drive has a bad command.	The Virtual Services Platform 9000 starts using factory defaults (if `boot config flags verify-config` is **`true`**, and a backup configuration is not specified).
The primary configuration file is specified. The configuration file on the flash drive has a bad command. The backup configuration file is specified, but it has a bad command.	The Virtual Services Platform 9000 fails the first configuration file, and starts ignoring the bad command.
The system is configured to start with factory defaults.	The Virtual Services Platform 9000 starts using factory defaults.

New software files

From the Avaya Support website, you can download all files simultaneously using the .tgz file.

For information about the name and size of software files, see *Release Notes for Avaya Virtual Services Platform 9000,* NN46250-401.

Checksums

The system performs internal checksums to ensure the integrity of the software.

Downgrade considerations

If you downgrade from a release, you need the previously saved configuration file (config.cfg) for the release to which you want to downgrade.

The Virtual Services Platform 9000 does not support different software versions running at the same time. For example, you cannot run Release 3.1 on the primary CP module and Release 3.0 on the secondary CP module.

If you disable the auto-commit feature and you do not commit an upgrade to gold within the specified commit time, the system automatically resets to the previous version. For more information about how commit to gold works, see Commit fundamentals on page 13.

Chapter 4: Administrative procedures

This chapter includes administrative procedures that you regularly use while upgrading, patching, or adding encryption modules to the Avaya Virtual Services Platform 9000. You can use these procedures to download patches and upgrades, or as part of normal system operations.

Downloading the software

Download new software to upgrade the Avaya Virtual Services Platform 9000. Software downloads can include encryption modules and software images.

Download patches and readme files from the Avaya support site at www.avaya.com/support.

Before you begin

- You must have access to the new software from the Avaya support site: www.avaya.com/support. You need a valid user or site ID and password.

About this task

Download the Advanced Encryption Standard (AES) and Data Encryption Standard (DES) software before you enable the encryption algorithms and use SNMPv3. The AES and DES encryption modules exist in a single file and you can enable them when the file is stored on flash.

Download the SSH encryption software before you enable the 3DES encryption module and use SSH.

Due to export restrictions, the encryption capability is separate from the main software image. SNMPv3 and the SSH server do not function properly without the use of this image.

For more information about file names for the current release, see *Release Notes for Avaya Virtual Services Platform 9000,* NN46250-401.

Important:

You must load the security encryption modules on the device before you can use the protocol.

Procedure

1. From an Internet browser, browse to www.avaya.com/support.
2. Click **DOWNLOADS**.
3. In the product search field, type **Virtual Services Platform 9000**.
4. In the **Choose Release** field, click a release number.

5. Click the download title to view the selected information.
6. Click the file you want to download.
7. Login to download the required software file.
8. Use an FTP client in binary mode to transfer the file to either the Virtual Services Platform 9000 or an external USB device.

Backing up configuration files

Before and after you upgrade your Avaya Virtual Services Platform 9000 software, make copies of the configuration files. If an error occurs, use backup configuration files to return the Virtual Services Platform 9000 to a previous state.

Avaya recommends that you keep several copies of backup files.

Before you begin

- If you use File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP), ensure that you enabled the FTP or TFTP server.
- You must log on to at least the Privileged EXEC mode in ACLI.

Procedure

1. Determine the configuration file names:

   ```
   show boot config choice
   ```

2. Save the configuration files. Assuming the files use the default file names, enter:

   ```
   save config
   ```

3. Save the configuration file to the secondary CP module if the SaveToStandby flag is false:

   ```
   save config standby config.cfg
   ```

4. Copy the files to a safe place:

   ```
   copy /intflash/config.cfg /extflash/config_backup.cfg
   ```

Backing up and restoring the compact flash to USB

Perform this procedure to back up and restore the contents of the internal or external compact flash to a USB flash device without entering multiple **copy** commands. This procedure is useful if you want to copy the complete compact flash contents to another chassis or want to replace the existing compact flash card or CP module without losing the data.

Before you begin

- You must have a USB storage device ready to use. Avaya supports USB 1 and 2. The memory size must be at least 2 GB. Avaya recommends that you use an Avaya USB storage device. For more information, see *Release Notes for Avaya Virtual Services Platform 9000,* NN46250-401.

About this task

The system verifies that the USB flash device has enough available space to perform the backup operation. If the USB flash device does not have enough available space, an error message appears. The backup command uses the following filepath on the USB flash device: `/usb/intflash/intflashbackup_yyyymmddhhmmss.tgz` and `/usb/extflash/extflashbackup_yyyymmddhhmmss.tgz`.

Logging is automatically disabled on the compact flash during backup.

The backup action can take up to 10 minutes.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Backup the internal flash to USB:

   ```
   backup intflash
   ```

3. Backup the external flash to USB:

   ```
   backup extflash
   ```

4. Restore the data to the internal flash:

   ```
   restore intflash
   ```

5. Restore the data to the external flash:

   ```
   restore extflash
   ```

6. Ensure that you enable logging for the external compact flash.

Example

```
VSP-9012:1#backup intflash
```

```
Warning: Internal flash is being used for logging right now.
       Backup/Restore intflash is not allowed. Please use the
       following CLI command in the global configuration mode
       to disable the logging to intflash, then try again.

 Case 1: If extflash is not present, disable the global logging.
       Command: no boot config flags logging

 Case 2: If extflash is present, enable logging to extflash.
       Command: logging logToExtFlash

 Execute  Command: logging logToExtFlash

 LoggingToPcmcia 1 LoggingToIntflash 0
```

```
Warning: Command will backup all data from /intflash to /usb/intflash.
         It will take a few minutes and may cause high CPU utilization.

         Are you sure you want to continue? (y/n) ? y

For file system /intflash:
          1934917632 total bytes on the filesystem
           643297280 used bytes on the filesystem
          1291620352 free bytes on the filesystem

For file system /usb:
          3990487040 total bytes on the filesystem
           499318784 used bytes on the filesystem
          3491168256 free bytes on the filesystem

cd /intflash ; /bin/tar -czvf /usb/intflash/intflashbackup_20110420212218.tgz * ; /bin/
sync

Info: Backup /intflash to filename /usb/intflash/intflashbackup_20110420212218.tgz is
complete!

         Do you want to stop the usb? (y/n) ? n

Logging to Intflash stopped

Logging to Extflash started
```

Configuring auto-commit

Use the auto-commit feature to let the system commit the software automatically after you install an upgrade or a patch, and after the commit timer expires. Configure the timer to give you enough time to verify the upgrade or patch does not cause a service impact. By default, the auto-commit feature is enabled with a timer of 10 minutes.

Before you begin

- You must log on to the Global configuration mode in ACLI.

Procedure

1. Enable auto-commit:

   ```
   sys software auto-commit enable
   ```

2. Configure the commit timer:

   ```
   sys software commit-time <10-60>
   ```

Variable definitions

Use the data in the following table to use the **`sys software`** command.

Variable	Value
auto-commit enable	Enables the auto-commit feature. The default is enabled. Use the no operator to disable auto-commit: **no sys software auto-commit enable**.
commit-time <*10-60*>	Configures the commit timer. The value is in minutes, between 10 and 60, with a default value of 10 minutes.

Disabling auto-commit

Disable the auto-commit feature to commit the upgrade or patch manually. Configure the timer to give you enough time to verify the upgrade or patch does not cause a service impact. By default, the auto-commit feature is enabled with a timer of 10 minutes. After the timer expires, the system verifies if you committed the upgrade or patch. If you did not commit the software or patch, the system reverts to the previous version. This feature protects the system from installing an upgrade or patch that causes service impact.

Before you begin

- You must log on to the Global configuration mode in ACLI.

Procedure

1. Disable auto-commit:

   ```
   no sys software auto-commit enable
   ```

2. Configure the commit timer:

   ```
   sys software commit-time <10-60>
   ```

Variable definitions

Use the data in the following table to use the **sys software** command.

Variable	Value
auto-commit enable	Enables the auto-commit feature. The default is enabled. Use the no operator to disable auto-commit: **no sys software auto-commit enable**.
commit-time <*10-60*>	Configures the commit timer. The value is in minutes, between 10 and 60, with a default value of 10 minutes.

Copying files

Copy files to back up files or to create a copy in another location.

Before you begin

- You must log on to at least the Privileged EXEC mode in ACLI.
- Using the **dir** command, ensure the required storage device has enough capacity before you copy a file to it.

Important:

If a failure occurs while you copy a file using FTP or TFTP (for example, if a TFTP server is not available), the destination file is deleted.

About this task

You can rename files while copying them. All procedures in this document use the default file names. You must use the right file names to ensure the upgrade is successful.

Procedure

Copy a file:

```
copy WORD<1-255> WORD<1-255>
```

Example

Copy config.cfg from the internal flash to the external flash on the CP module to which you are connected:

```
VSP-9012:1#copy /intflash/config.cfg /extflash/config_backup.cfg
```

Copy an image or configuration file from the FTP server to the internal flash on the CP module to which you are connected:

```
VSP-9012:1#copy 111.111.1.11:config.cfg /intflash/config.cfg
```

Copy config.cfg from the internal flash on the CP module to which you are connected to the external flash on the CP module to which you are not connected:

```
VSP-9012:1#copy /intflash/config.cfg /mnt/extflash/config_backup.cfg
```

Variable definitions

Use the data in the following table to use the **copy** command.

Variable	Value
WORD<1-255>	The first instance specifies the source path and name of the file the system will copy from. The second instance specifies the destination path and name of the copy the system will create.

Comments? infodev@avaya.com

Variable	Value
	The correct syntax can be one of the following: • a.b.c.d: <file> • /intflash/<file> Use this option for the internal flash of the CP module to which you are connected. • /extflash/<file> Use this option for the external flash of the CP module to which you are connected. • /usb/<file> • /mnt/intflash/<file> Use this option for the internal flash of the CP module to which you are not connected. • /mnt/extflash/<file> Use this option for the external flash of the CP module to which you are not connected.

Determining available storage space

Determine whether the Avaya Virtual Services Platform 9000 has enough storage space to store the new software.

Before you begin

- You must log on to at least the Privileged EXEC mode in ACLI.

Important:

You need the older configuration files if the upgrade is unsuccessful. Ensure you back up these files to a safe place before you remove them.

Procedure

1. View the free space and files in the internal flash memory:

   ```
   dir
   ```

   The bottom of the table shows available space, for example:

   ```
   total: 2971209728 used: 2441273344 free: 529936384 bytes
   ```

2. If you must remove files to make space, use the **remove** command:

   ```
   remove WORD<1-99> [-y]
   ```

Variable definitions

Use the data in the following table to help you use the **remove** command.

Variable	Value
WORD<1-99>	Specifies the file to remove.
-y	Skips the confirm question.

Enabling FTP and TFTP

Enable File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) to use these protocols to transfer files on the Avaya Virtual Services Platform 9000 to transfer files.

Before you begin

- You must log on to the Global Configuration mode in ACLI.

Procedure

1. Enable the FTP server:

   ```
   boot config flags ftpd
   ```

   OR

   Enable the TFTP server:

   ```
   boot config flags tftpd
   ```

2. Save the configuration file:

   ```
   save config
   ```

3. Save the configuration file to the secondary CP module if the SaveToStandby flag is false:

   ```
   save config standby config.cfg
   ```

4. Restart the Virtual Services Platform 9000 with the FTP or TFTP server active:

   ```
   boot
   ```

Specifying configuration file sources

Perform this procedure to configure the names and locations of the primary and backup configuration files.

Before you begin

- You must log on to the Global Configuration mode in ACLI.

Procedure

Set the primary and backup configuration files:

```
boot config choice primary {config-file WORD<0-255>|backup-config-file
WORD<0-255>}
```

Example

Assign the primary configuration file:

```
VSP-9012:1(config)#boot config choice primary config-file /intflash/
primaryconfig.cfg
```

Assign the backup configuration file:

```
VSP-9012:1(config)#boot config choice primary backup-config-file /
extflash/primarybackupconfig.cfg
```

Variable definitions

Use the data in the following table to use the **`boot config choice primary`** command.

Variable	Value
backup-config-file *WORD<0-255>*	Specifies the backup boot configuration file; *WORD<0-255>* is the path and file name, up to 255 characters.
config-file *WORD<0-255>*	Specifies the boot configuration file; *WORD<0-255>* is the path and file name, up to 255 characters.

Chapter 5: Software upgrade

Upgrade the Avaya Virtual Services Platform 9000 to add functionality.

Before you begin

- For more information about upgrade times, see Upgrade time requirements on page 11. If necessary, schedule a time for the Virtual Services Platform 9000 to be nonoperational.

Caution:

Risk of service interruption

If the Virtual Services Platform 9000 routes a high rate of traffic during the upgrade process, you can notice some performance impact during the upgrade. Try to perform upgrades during off-peak periods.

Important:

All upgrade procedures assume that you use default file names. Use caution while you perform a procedure if you use nondefault file names. Ensure that all parameters associated with file names take into consideration the use of the nondefault values.

Upgrading the software

Perform this procedure to upgrade the software on the Avaya Virtual Services Platform 9000. This procedure shows how to upgrade the software using the internal flash memory as the file storage location; you can use other storage locations.

Before you begin

- Back up the configuration files.
- Download the upgrade file to the Virtual Services Platform 9000.
- Avaya Virtual Services Platform 9010 supports two upgrade paths:
  - Release 3.3.3.x to Release 4.0.
  - Release 3.4.x to Release 4.0.
- Avaya Virtual Services Platform 9012: No restrictions exist for the upgrade. For Avaya Virtual Services Platform 9012, you can upgrade directly to Release 4.0. You do not need to install Release 3.3.3.0 or later prior to upgrading to Release 4.0.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Extract the release distribution files to the `/intflash/release/` directory:

   ```
   software add WORD<1-99>
   ```

3. Install the image:

   ```
   software activate WORD<1-99>
   ```

4. Restart the Virtual Services Platform 9000:

   ```
   reset
   ```

   Important:

   After you restart the system, you have the amount of time configured for the commit timer to verify the upgrade and commit the software to gold. If you do not commit the software to gold and you did not enable auto-commit, the system restarts with the last known working version after the commit timer expires. This feature ensures you can regain control of the system if an upgrade fails.

5. Confirm the software upgrade:

   ```
   show software [verbose]
   ```

Example

The following figures show detailed examples of the **`show software`** and **`show software verbose`** commands throughout the various stages of the upgrade process, such as **`software add`**, **`software activate`**, and **`software commit`** (manual and auto). The following example shows a software upgrade from Release 3.3.1.1 to Release 3.4.

Software add:

In the following two examples, note that Release 3.4.0.0.GA now appears in the output. The **`show software verbose`** output also shows the Committed Type as Not Committed.

```
VSP-9012:1(config)#software add VSP9K.3.4.0.0.tgz

VSP-9012:1(config)#show software

================================================================================
                software releases in /intflash/release/
================================================================================
3.1.0.0.GA
3.2.0.0.GA
3.3.0.0.GA (Backup Release)
3.3.1.1.GA (Primary Release)
3.4.0.0.GA
--------------------------------------------------------------------------------
Auto Commit     : enabled
Commit Timeout  : 10 minutes
```

```
VSP-9012:1(config)#show software verbose

================================================================================
                software releases in /intflash/release/
================================================================================
================================================================================
Release                Added Time      Activated Time    Committed Time    Committed Type
================================================================================
3.1.0.0.GA             --------        --------          --------          --------
3.2.0.0.GA             --------        --------          --------          --------
3.3.0.0.GA             --------        --------          --------          --------
(Backup Release)
3.3.1.1.GA             --------        --------          --------          --------
(Primary Release)
3.4.0.0.GA             --------        --------          --------          Not Committed
--------------------------------------------------------------------------------

Auto Commit     : enabled
Commit Timeout  : 10 minutes
```

Software activate:

In the following two examples, note that Release 3.4.0.0.GA is now shown as the Next Boot Release.

```
VSP-9012:1(config)#software activate 3.4.0.0.GA

VSP-9012:1(config)#show software

================================================================================
            software releases in /intflash/release/
================================================================================
3.1.0.0.GA
3.2.0.0.GA
3.3.0.0.GA
3.3.1.1.GA (Primary Release)
3.4.0.0.GA (Next Boot Release)

--------------------------------------------------------------------------------
Auto Commit     : enabled
Commit Timeout  : 10 minutes
```

```
VSP-9012:1(config)#show software verbose

================================================================================
            software releases in /intflash/release/
================================================================================
================================================================================================
Release                 Added Time          Activated Time      Committed Time      Committed Type
================================================================================================
3.1.0.0.GA              --------            --------            --------            --------
3.2.0.0.GA              --------            --------            --------            --------
3.3.0.0.GA              --------            --------            --------            --------
3.3.1.1.GA              --------            --------            --------            --------
(Primary Release)
3.4.0.0.GA              --------            --------            --------            Not Committed
(Next Boot Release)

--------------------------------------------------------------------------------

Auto Commit     : enabled
Commit Timeout  : 10 minutes
```

After a system restart:

In the following two examples, note that Release 3.4.0.0.GA is now shown as the Primary Release. The auto-commit timer shows the remaining time before an auto-commit. The **`show software verbose`** output shows the timestamps for the Added Time and Activated Time.

```
VSP-9012:1(config)#show software

================================================================================
            software releases in /intflash/release/
================================================================================
3.1.0.0.GA
3.2.0.0.GA
3.3.0.0.GA
3.3.1.1.GA (Backup Release)
3.4.0.0.GA (Primary Release)

--------------------------------------------------------------------------------
Auto Commit     : enabled
Commit Timeout  : 10 minutes
Remaining time until software auto-commit is 9 minutes 27 seconds
```

```
VSP-9012:1(config)#show software verbose
================================================================================
            software releases in /intflash/release/
================================================================================
================================================================================
Release                 Added Time          Activated Time      Committed Time      Committed Type
================================================================================
3.1.0.0.GA              -------             -------             -------             -------
3.2.0.0.GA              -------             -------             -------             -------
3.3.0.0.GA              -------             -------             -------             -------
3.3.1.1.GA              -------             -------             -------             -------
(Backup Release)
3.4.0.0.GA              2013-04-21 07:02:27 2013-04-21 07:11:10 -------             Not Committed
(Primary Release)
--------------------------------------------------------------------------------

Auto Commit     : enabled
Commit Timeout  : 10 minutes
Remaining time until software auto-commit is 9 minutes 27 seconds
```

Manual and automatic software commit:

The following example shows the **`show software verbose`** output for a manual software commit. The Committed Time timestamp appears and the Committed Type shows as Manual.

```
VSP-9012:1(config)#software commit
VSP-9012:1(config)#show software verbose
================================================================================
                software releases in /intflash/release/
================================================================================
================================================================================================
Release                 Added Time          Activated Time      Committed Time      Committed Type
================================================================================================
3.1.0.0.GA              -------             -------             -------             -------
3.2.0.0.GA              -------             -------             -------             -------
3.3.0.0.GA              -------             -------             -------             -------
3.3.1.1.GA              -------             -------             -------             -------
(Backup Release)
3.4.0.0.GA              2013-04-21 07:02:27 2013-04-21 07:11:10 2013-04-21 07:21:15 Manual
(Primary Release)

------------------------------------------------------------------------------

Auto Commit     : enabled
Commit Timeout  : 10 minutes
```

The following example shows the **show software verbose** output for an automatic software commit after the 10 minute commit timer expired. The Committed Time timestamp appears and the Committed Type shows as Auto.

```
VSP-9012:1(config)#show software verbose

================================================================================
                software releases in /intflash/release/
================================================================================
================================================================================================
Release                 Added Time          Activated Time      Committed Time      Committed Type
================================================================================================
3.1.0.0.GA              -------             -------             -------             -------
3.2.0.0.GA              -------             -------             -------             -------
3.3.0.0.GA              -------             -------             -------             -------
3.3.1.1.GA              -------             -------             -------             -------
(Backup Release)
3.4.0.0.GA              2013-04-21 07:02:27 2013-04-21 07:11:10 2013-04-21 07:26:15 Auto
(Primary Release)

------------------------------------------------------------------------------

Auto Commit     : enabled
Commit Timeout  : 10 minutes
```

All releases prior to Release 3.4 do not show a timestamp in the **show software verbose** command output regardless of whether you add, activate, or commit. When upgrading from releases prior to Release 3.4, the Added Time and Activated Time timestamps appear after a system restart and you only see the timestamps for Release 3.4 and later.

Note:

For upgrades post Release 3.4, you do not need to restart the system to see the updated timestamps for Added Time and Activated Time. The timestamps immediately appear in **show software verbose** output after you issue the commands **software add** and **software activate**.

Variable definitions

Use the data in the following table to use the **software** command.

Variable	Value
activate *WORD<1-99>*	Specifies the name of the software release image.
add *WORD<1-99>*	Specifies the path and version of the compressed software release archive file.
remove *WORD<1-99>*	Specifies the path and version of the compressed software release archive file.

Verifying the upgrade

Verify your upgrade to ensure proper Avaya Virtual Services Platform 9000 operation.

Procedure

1. Check for alarms or unexpected errors:

   ```
   show logging file tail
   ```

2. Verify all modules and slots are online:

   ```
   show sys-info
   ```

Committing an upgrade

Perform the following procedure to commit an upgrade.

About this task

The commit function for software upgrades allows maximum time set by the commit timer (the default is 10 minutes) to ensure that the upgrade is successful. If you enable the auto-commit option, the system automatically commits to the new software version after the commit timer expires. If you disable the auto-commit option, you must issue the software commit command before the commit timer expires to commit the new software version, otherwise the system restarts automatically to the previous (committed) version.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. **(Optional)** Extend the time to commit the software:

```
software reset-commit-time [<1-60>]
```

3. Commit an upgrade:

```
software commit
```

Downgrading the software

Perform this procedure to downgrade the Avaya Virtual Services Platform 9000 from the current trusted version to a previous release.

Before you begin

Ensure that you have a previous version installed.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Activate a prior version of the software:

```
software activate WORD<1-99>
```

3. Restart the Virtual Services Platform 9000:

```
reset
```

Important:

After you restart the system, you have the amount of time configured for the commit timer to verify the software change and commit the software to gold. If you do not commit the software to gold and auto-commit is not enabled, the system restarts with the last known working version after the commit timer expires. This feature ensures you can regain control of the system if an upgrade fails.

4. Commit the software change:

```
software commit
```

Important:

If you do not enable the auto-commit functionality, you must commit the software change before the commit timer expires. This is an optional step otherwise.

5. Verify the downgrade:
   - Check for alarms or unexpected errors using the `show logging file tail` command.
   - Verify all modules and slots are online using the `show sys-info` command.
6. (Optional) Remove unused software:

```
software remove WORD<1-99>
```

Variable definitions

Use the data in the following table to use the **software** command.

Variable	Value
activate *WORD<1-99>*	Specifies the name of the software release image.
add *WORD<1-99>*	Specifies the path and version of the compressed software release archive file.
remove *WORD<1-99>*	Specifies the path and version of the compressed software release archive file.

Performing a VSP 9000 network hitless upgrade

VSP 9000 cluster switches can be hitless upgraded. VSP 9000 provides hardware-assisted switch clustering (SMLT). The benefit of this is that a flow of traffic can fail over to the peer switch in sub 20ms during a link failure or a switch restart. Failover time also depends on the SMLT-attached switches link failure detection capabilities.

Review the entire upgrade procedure to ensure that you clearly understand all of the steps and collect any required information about port assignments before you proceed with the upgrade. If you are unclear on any of the procedure steps, contact Avaya Technical Support before you proceed with the upgrade.

Before you begin

- You have transferred the new software files to both nodes.
- Ensure that you have access to both systems. Avaya recommends that you perform this upgrade by using a console cable or by using access through the out-of-band management Ethernet port. If you have inband access only, and your session flows over a non-SMLT connected port, ensure that you do not shut down the port that you use to perform the upgrade procedure.

About this task

When you upgrade a pair of core switches that connect through an IST peer connection, you must take special care. If you are upgrading a cluster from Release 3.0.0.0 , see wi00859221 in the Release Notes for further details. wi00859221 was resolved in Release 3.1 and is documented in *Release Notes for Avaya Virtual Services Platform 9000,* NN46250-401.

Perform this procedure to upgrade the two peer switches and minimize the network downtime. The following figure shows two switches that use an IST peer connection. In the example, the following ports are the SMLT ports:

- SMLT 1 uses ports 4/2, 4/14, 4/26, 4/38.
- SMLT 4 uses ports 4/13, 4/25, 4/37.
- SMLT 500 uses port 4/47.

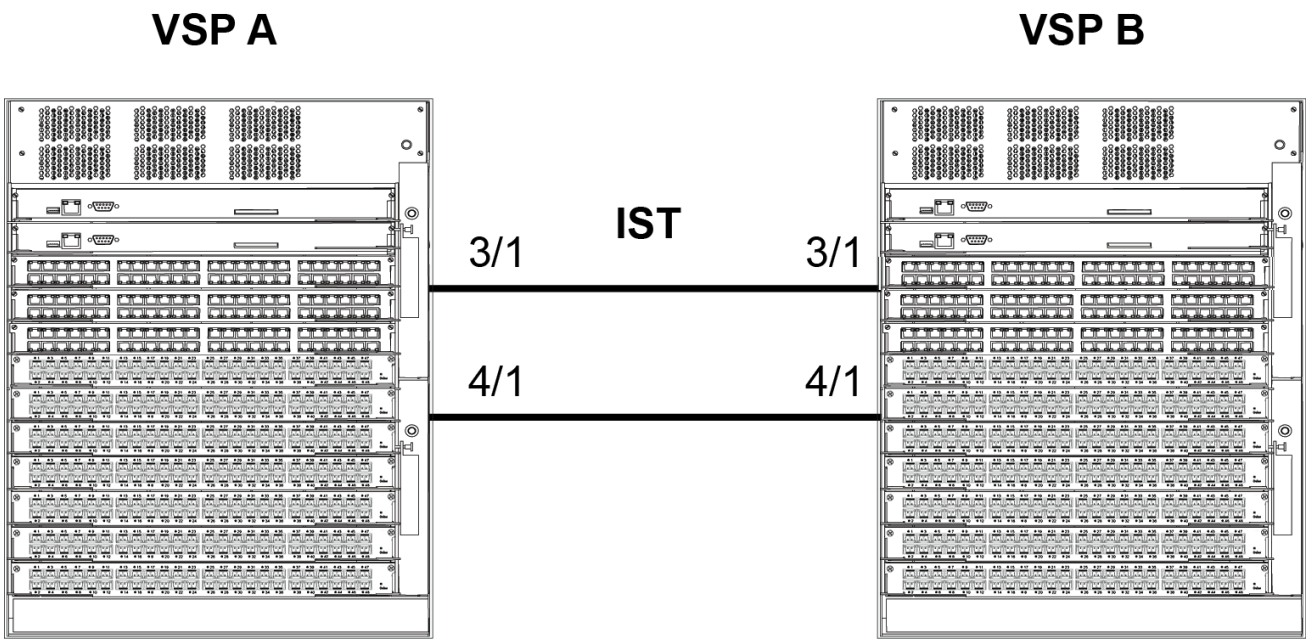


Figure 1: IST peer configuration

Procedure

1. Log on to the console ports for each device.
2. Save the running configuration to ensure that it is correctly retrieved after you reset the systems:

   ```
   save config
   ```

3. Add the software release on both nodes of the cluster:

   ```
   software add VSP9K.3.4.0.0.tgz
   ```

   ```
   software add-modules 3.4.0.0.GA VSP9K.3.4.0.0_modules.tgz
   ```

4. Activate the software release on both nodes of the cluster:

   ```
   software activate 3.4.0.0.GA
   ```

5. On the first device, to force all traffic to the switch that you are not upgrading, shut down all SMLT ports, leaving the IST ports up.

   Note:

   Do not save the configuration after you disable the ports.

   ```
   enable
   ```

   ```
   config t
   ```

   ```
   int gig 4/2,4/14,4/26,4/38,4/13,4/25,4/37,4/47
   ```

   ```
   shutdown
   ```

Note:

For simplicity, you can also shut down all non-IST ports on the system, however, this will cause systems that connect by using non-SMLT ports to experience a longer outage as you complete the upgrade procedure. You can obtain a list of SMLT ports by using the `show mlt` command, and noting the port members from all MLTs where the `MLT ADMIN` column shows `smlt`.

6. Verify that SMLT traffic has switched over to the SMLT cluster peer node.
7. Reset the first device:

   ```
   reset –y
   ```

   The device resets and starts in approximately 3–4 minutes.
8. After the device starts, log on with read and write privileges to commit the software:

   ```
   enable
   software commit
   ```

   The first VSP 9000 now runs the new software version. The SMLT ports on the first node will be locked and physically link down while the IST channel attempts to establish a connection to the peer node. After approximately 60 seconds, the SMLT ports on the first node will automatically unlock and come back up.

   Important:

   You must wait for the ports to unlock and come back up before you proceed to the next step of this procedure. Failure to wait will result in traffic loss.

   Perform the remaining procedure steps on the second device.
9. On the second device, to force all traffic to the now upgraded switch, shut down all SMLT ports, leaving the IST ports up.

   Note:

   In this example, the SMLT port assignments are the same on VSP A and VSP B. The port numbers may differ between the peer nodes in your configuration.

   ```
   enable
   config t
   int gig 4/2,4/14,4/26,4/38,4/13,4/25,4/37,4/47
   shutdown
   ```

   Note:

   For simplicity, you can also shut down all non-IST ports on the system, however, this will cause systems that connect by using non-SMLT ports to experience a longer outage as you complete the upgrade procedure. You can obtain a list of SMLT ports by using the `show mlt` command, and noting the port members from all MLTs where the `MLT ADMIN` column shows `smlt`.

10. Verify that SMLT traffic has switched over to the SMLT cluster peer node.
11. Reset the second device:

    ```
    reset –y
    ```

    The device resets and starts in approximately 3–4 minutes.
12. After the device starts, log on with read and write privileges to commit the software:

    ```
    enable
    ```

    ```
    software commit
    ```

    After the restart, both devices use the same version of software and IST channel. The IST channel is reestablished and SMLTs return to a working state.
13. Verify the IST state for the IST channel is up:

    ```
    show ist mlt
    ```

```
================================================================================
                                  Mlt IST Info
================================================================================
MLT   PEER-IP              VLAN     ENABLE   IST
ID    ADDRESS              ID       IST      STATUS
--------------------------------------------------------------------------------
2    10.254.172.2          172      true     up


NEGOTIATED                                    MASTER/
DIALECT      IST STATE                        SLAVE
--------------------------------------------------------------------------------
v1.0         Up                               Slave
```

14. Verify the current state of the IST and active SMLTs. The following example shows only partial command output.

    ```
    show mlt
    ```

```
================================================================================
                                    Mlt Info
================================================================================
                          PORT    MLT   MLT        PORT         VLAN
MLTID IFINDEX NAME        TYPE    ADMIN CURRENT    MEMBERS      IDS
--------------------------------------------------------------------------------
1   6144  SMLT-1        trunk   smlt   smlt     4/2,4/14,4/26,4/38
2 3 4
2   6145  IST-MLT       trunk   ist    ist      3/1, 4/1
2 3 4 172 200 500
4   6147  SMLT-4        trunk   smlt   smlt     4/13,4/25,4/37  4
100 6243  MLT-100       trunk   norm   norm     4/23-4/24,4/27-4/28
100
500 6643  SMLT-500      trunk   smlt   norm     4/47              500

All 5 out of 5 Total Num of mlt displayed
```

Chapter 6: Software patch

Before you begin

- Review the readme file for the patch.

Important:

All patching procedures assume that you use default file names. Use caution while you perform a procedure if you use nondefault file names. Ensure that all parameters associated with file names take into consideration the use of the nondefault values.

About this task

The following task flow shows the patch application and patch removal process.

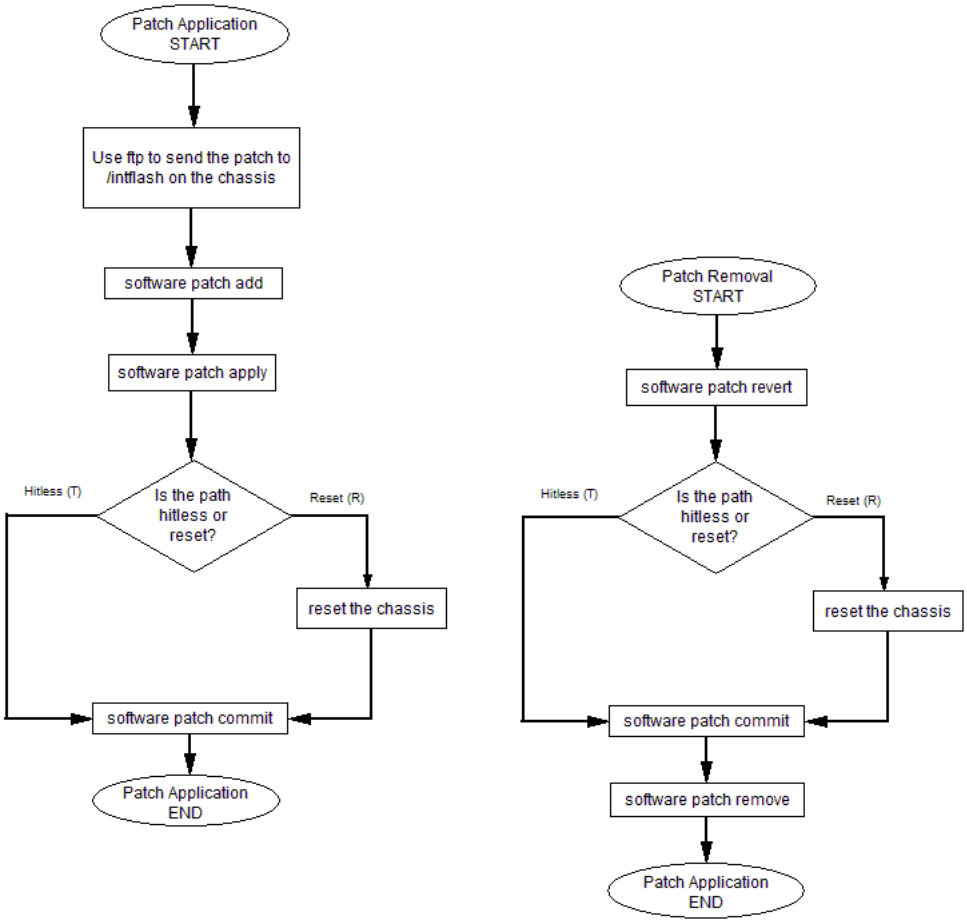


Figure 2: Patch application and removal

The following task flow demonstrates the steps involved in committing a software patch.

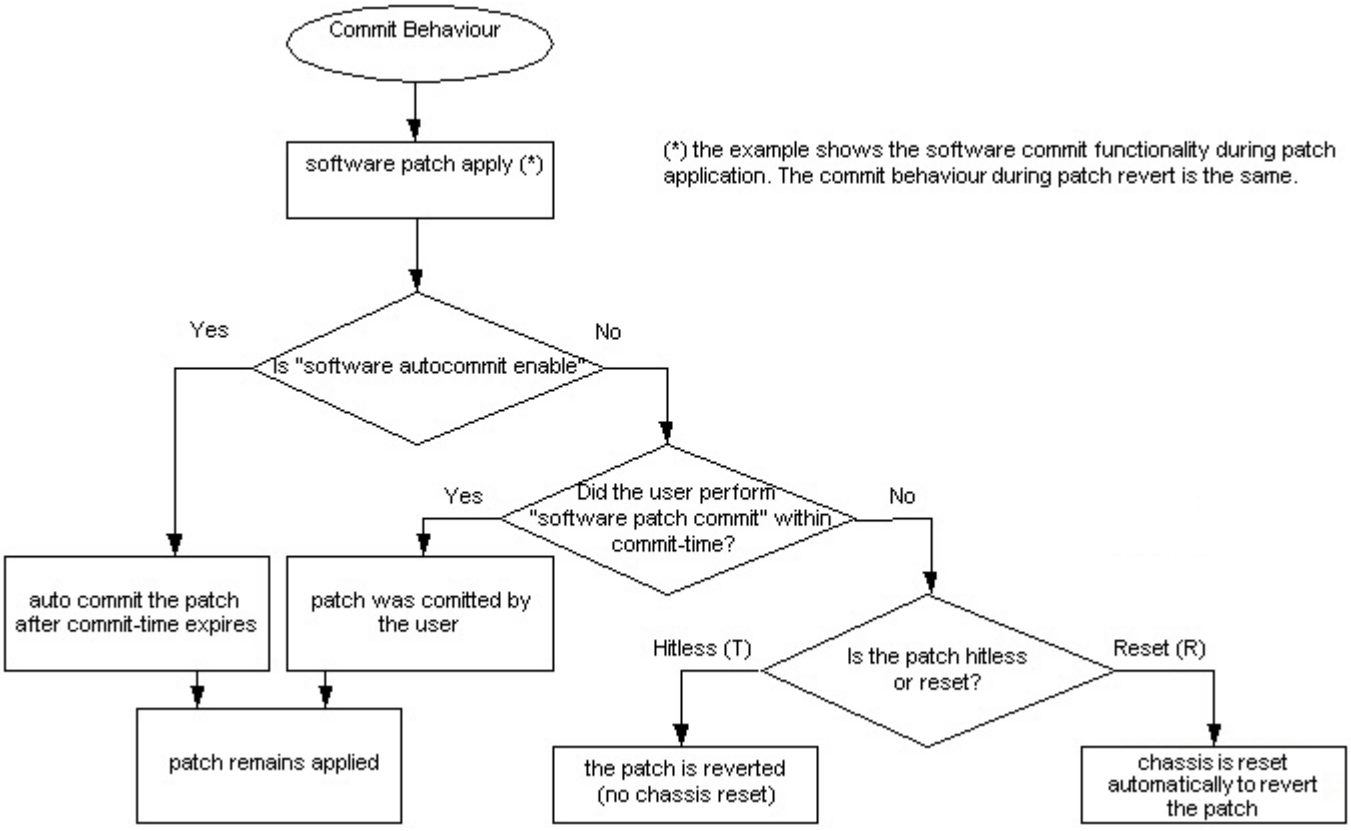


Figure 3: Committing a software patch

Patching the software

Patch the software to fix and correct a problem in software code, its supporting data, or update a feature. If you enable the auto-commit feature, the system commits the patch automatically after the commit timer expires. If you disable the auto-commit feature, you must commit the patch manually before the commit timer expires.

Before you begin

- Download the patch file in binary format to the Virtual Services Platform 9000.
- Ensure you are familiar with the commit and auto-commit features. For more information about commit, see Commit fundamentals on page 13.

Procedure

1. Uncompress the patch and add it to the patch database:

   ```
   software patch add WORD<1-255>
   ```

2. Activate the patch functionality:

```
software patch apply patch-ids WORD<1-255> [WORD<1-255>]
```

Important:

After you apply the patch, the system begins the commit timer. Use that time to verify the patch before you commit the patch.

Important:

After you apply a reset patch, you must restart the system to allow the patch functionality to take effect.

Example

1. Uncompress the patch and add it to the patch database:

```
VSP-9012:1# software patch add VSP9K.3.0.0.0-T00734412A.tgz
```

```
 Unpacking patch T00734412A for software version VSP9K.3.0.0.0 to /intflash/
release/VSP9K.3.0.0.0/patches/T00734412A
Unpacking of T00734412A software version VSP9K.3.0.0.0 to /intflash/release/VSP9K.
3.0.0.0/patches/T00734412A is successful.
Setting permission on /intflash/release/VSP9K.3.0.0.0/patches/T00734412A is
successful.
```

2. Activate the patch functionality:

```
VSP-9012:1# software patch apply patch-ids T00734412A
```

```
 Checking relationships and calculating order of application.

The following patches will be applied in the order listed:
Identifier    Status     Title
T00734412A     candidate  VSP9000:EDM-saveRuntimeConfigToSlave Causes Error on
Slave
Requesting permission to proceed from Software Control
Applying patch T00734412A PA on slot 4
Applying patch T00734412A PA on slot 1
Applied patches with the following results:
Identifier     Result     Cause
T00734412A     success    patch applied
Patch activation will automatically be committed in 10 minutes unless a rollback
is requested.
Success
```

3. Commit the software patch:

```
VSP-9012:1# software patch commit
```

```
Committing patch activation with Software Control
Patch request committed - rollback will not occur.
Success
```

Variable definitions

Use the data in the following table to use the **`software patch`** command.

Variable	Value
add *WORD<1-255>*	Specifies the path and version of the compressed software patch archive file.
apply {all|hitless|patch-ids *WORD<1-255> [WORD<1-255>]* |reset}	Activates the patch functionality. • all: activates patch functionality of patches in the Candidate (ca) state. • hitless: activates all hitless patches in the Candidate (ca) state. • patch-ids *WORD<1-255> [WORD<1-255>]*: installs specific patches. You can specify up to eight patches at a time. The ID is the same as the patch file name without the -version.tgz extension. • reset: activates all reset patches in the Candidate (ca) state.

Verifying the patch

Verify the patch to ensure your Avaya Virtual Services Platform 9000 operates properly after the patch installation and that the patch did not cause a service impact.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Verify that the patch installation is complete:

   ```
   show software patch
   ```

3. Check for alarms or unexpected errors:

   ```
   show logging file tail
   ```

Committing a patch

If you disabled the auto-commit feature, you must manually commit the patch after you verify that a patch does not cause a service impact. After the commit timer expires, the system removes any patch that was not committed manually.

If you applied a reset patch, you must commit the patch after the system restarts. After the commit timer expires, the system removes any patch that was not committed and restarts.

About this task

Caution:

During Telnet sessions only, when issuing the **software patch commit** or **software patch remove** commands, the message to indicate the CPUs are synchronizing does not appear and a command prompt is returned before synchronization completes. Synchronizing can take several minutes. Do not issue another command until you see the prompt that synchronization is complete. This caution does not apply to console sessions.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. **(Optional)** Extend the time to apply the patch:

   ```
   software reset-commit-time [<1–60>]
   ```

3. Commit the patch:

   ```
   software patch commit
   ```

Removing a patch

Remove a patch from the Avaya Virtual Services Platform 9000 if the patch causes problems.

About this task

Caution:

Deficiency when using telnet to commit or remove a patch on an HA CPU (WI00511642 to be resolved in the next release).

The HA sync can take 2 minutes depending upon the level of configuration present. When you use the console to commit or remove a patch a message like *Syncing release directory on backup CP card in slot 2*appears on the console and the console prompt holds until the process is complete at which time a message like *Syncing release directory on backup CP card in slot 2 completed* appears and the prompt returns. The message only appears on the console screen. No message appears on the Telnet session, which can cause the user to think there is something wrong because the session seems to hang until the CPUs have synchronized. Also, while the two CPU are synchronizing, the user can not issue commands in the current Telnet session until the synchronize action is complete.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Revert the patch:

   ```
   software patch revert patch-ids WORD<1-255>
   ```

3. Commit the software patch revert action

   ```
   software patch commit
   ```

4. Remove the patch from the system.

   ```
   software patch remove version WORD<1-255> patch-id WORD<1-255>
   ```

Example

1. Revert the patch:

   ```
   VSP-9012:1# software patch revert patch-ids T00734412A
   ```

   ```
   Checking relationships and calculating order of application.
    The following patches will be removed in the order listed:
       Identifier    Status     Title
   T00734412A     applied    VSP9000:EDM-saveRuntimeConfigToSlave Causes
   Error on Slave Requesting permission to proceed from Software Control
   Removing patch T00734412A PA on slot 4
   Removing patch T00734412A PA on slot 1
   Removed patches with the following results:
   Identifier    Result     Cause
   T00734412A     success    patch removed
   Patch activation will automatically be committed in 10 minutes unless a rollback
   is requested.
   Success
   ```

2. Commit the software patch revert action.

   ```
   VSP-9012:1# software patch commit
   ```

3. Remove the patch from the `/intflash/release/<version>/patches/<patch-id>` directory and from the patch database:

   ```
   VSP-9012:1# software patch remove version VSP9K.3.0.0.0 patch-id
   T00734412A
   ```

   ```
    Patch T00734412A for swVersion VSP9K.3.0.0.0 is removed successfully.
   ```

Variable definitions

Use the data in the following table to use the **`software patch`** command.

Variable	Value
revert {all|hitless|patch-ids *WORD<1-255>* *[WORD<1-255>* |reset} [version <software_version>]	Deactivates the specified patch.
remove version *WORD<1-255>* patch-id *WORD<1-255>*	Removes the patch from the system.

Aborting a patch

If adding or reverting a patch causes a service impact, and the commit timer has not yet expired; you can abort the addition or reversion process.

Important:

Aborting a reset patch causes the system to restart.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Abort a patch:

   ```
   software patch abort
   ```

   Important:

   You can only abort a reset patch after the system restarts.

Chapter 7: Encryption module installation

Add encryption modules to the Avaya Virtual Services Platform 9000 software to use the encryption features.

Before you begin

Important:

This chapter assumes that you use default file names. Use caution while performing a procedure if you use nondefault file names. Ensure that all parameters associated with file names take into consideration the use of the nondefault values.

Adding an encryption module

You can add encryption modules to a software release to use encryption features.

Before you begin

- Download the module file to the Avaya Virtual Services Platform 9000.
- You must log on to at least the Privileged EXEC mode in ACLI.

Procedure

1. Add an encryption module to a release version:

   ```
   software add-modules WORD<1-99> WORD<1-99>
   ```

2. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

3. Load the encryption module:

   ```
   load-encryption-module {3DES|AES|DES}
   ```

Example

Add the Advanced Encryption Standard (AES) module to the Release 3.4:

```
VSP-9012:1#software add-modules 3.4.0.0.GA VSP9K.3.4.0.0_modules.tgz
```

Log on to Global Configuration mode:

```
VSP-9012:1#configure terminal
```

Load the AES encryption module:

```
VSP-9012:1(config)#load-encryption-module AES
```

Variable definitions

Use the data in the following table to use the **`software add-modules`** command.

Variable	Value
The first *WORD<1-99>*.	Specifies the release version to which you want to add modules to.
The second *WORD<1-99>*.	Specifies the module archive you want to add.

Use the data in the following table to use the **`load-encryption-module`** command.

Variable	Value
<3DES|AES|DES>	Specifies the encryption module to load.

Chapter 8: Translations of safety messages

This section contains translations of caution, warning, and danger messages that appear in the documentation.

Class A electromagnetic interference warning statement

Warning:

Risk of electromagnetic interference

This device is a Class A product. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users are required to take appropriate measures necessary to correct the interference at their own expense.

Warning:

AVERTISSEMENT

Le périphérique est un produit de Classe A. Le fonctionnement de cet équipement dans une zone résidentielle risque de causer des interférences nuisibles, auquel cas l'utilisateur devra y remédier à ses propres frais.

Warning:

WARNUNG

Dies ist ein Gerät der Klasse A. Bei Einsatz des Geräts in Wohngebieten kann es Störungen des Radio- und Fernsehempfangs verursachen. In diesem Fall muss der Benutzer alle notwendigen Maßnahmen ergreifen, die möglicherweise nötig sind, um die Störungen auf eigene Rechnung zu beheben.

Warning:

ADVERTENCIA

Este es un producto clase A. El uso de este equipo en áreas residenciales puede causar interferencias nocivas, en cuyo caso, se requerirá que los usuarios tomen cualquier medida necesaria para corregir la interferencia por cuenta propia.

Warning:

AVISO

Este dispositivo é um produto Classe A. Operar este equipamento em uma área residencial provavelmente causará interferência prejudicial; neste caso, espera-se que os usuários tomem as medidas necessárias para corrigir a interferência por sua própria conta.

Warning:

AVVISO

Questo dispositivo è un prodotto di Classe A. Il funzionamento di questo apparecchio in aree residenziali potrebbe causare interferenze dannose, nel cui caso agli utenti verrà richiesto di adottare tutte le misure necessarie per porre rimedio alle interferenze a proprie spese.

Electrostatic discharge caution statement

Electrostatic alert:

ELECTROSTATIC ALERT

ESD can damage electronic circuits. Do not touch electronic hardware unless you wear a grounding wrist strap or other static-dissipating device.

Electrostatic alert:

ELEKTROSTATIKWARNUNG

Elektronische Schaltkreise können durch elektrostatische Entladung beschädigt werden. Berühren Sie elektronische Hardware nur, wenn Sie ein Erdungsarmband oder ein anderes Statik ableitendes Medium tragen.

Electrostatic alert:

ALERTA DE ELECTROESTÁTICA

Una descarga electroestática puede dañar los circuitos eléctrónicos. No toque el hardware electrónico a no ser que utilicé una muñequera antiestática u otro dispositivo disipador de estática.

Electrostatic alert:

ALERTA CONCERNANT LES DÉCHARGES ÉLECTROSTATIQUES

Une décharge électrostatique (DES) peut endommager les circuits électroniques. Ne touchez pas le matériel électronique, à moins de mettre à votre poignet une bande de mise à la masse ou autre dispositif dissipant l'électricité statique.

Electrostatic alert:

ALERTA DE ELETROSTÁTICA

ESD pode danificar circuitos eletrônicos. Não toque em equipamentos eletrônicos a menos que esteja utilizando pulseira de aterramento ou outro dispositivo para dissipação de energia estática.

Electrostatic alert:

AVVISO ELETTROSTATICO

Le scariche elettrostatiche (ESD) possono danneggiare i circuiti elettronici. Non toccare i componenti elettronici senza aver prima indossato un braccialetto antistatico o un altro dispositivo in grado di dissipare l'energia statica.

Glossary

Advanced Encryption Standard (AES)	A privacy protocol the U.S. government organizations use AES as the current encryption standard (FIPS-197) to protect sensitive information.
Electrostatic Discharge (ESD)	The discharge of stored static electricity that can damage electronic equipment and impair electrical circuitry that results in complete or intermittent failures.
Trivial File Transfer Protocol (TFTP)	A protocol that governs transferring files between nodes without protection against packet loss.