



Send document comments to nexus1k-docfeedback@cisco.com.



Cisco Nexus Virtual Services Appliance Software Installation and Upgrade Guide, Release 4.2(1) SP1(5.1)

September 10, 2014

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-27729-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Nexus Virtual Services Appliance Software Installation and Upgrade Guide, Release 4.2(1) SPI(5.1)
© 2010-2012 Cisco Systems, Inc. All rights reserved.

Send document comments to nexus1k-docfeedback@cisco.com.



CONTENTS

Audience	v
Recommended Reading	v
Organization	vi
Document Conventions	vi
Related Documentation	vii
Obtaining Documentation and Submitting a Service Request	ix
	ix

Overview 1-1

Information About Cisco Nexus Virtual Services Appliance	1-1
Cisco Integrated Management Controller	1-1
Supported PIDs for Cisco Nexus Virtual Services Appliance Product Family	1-2
Software Included	1-2
Flow Chart: Installing and Configuring the Cisco Nexus Virtual Services Appliance	1-3
Additional References	1-6

Cisco Nexus Virtual Services Appliance Software Installation 2-1

Information About Software Install	2-1
Prerequisites	2-2
Guidelines and Limitations	2-2
Cisco Host Upgrade Utility Information	2-3
Verifying the CIMC Software Version	2-4
Gathering Information About the Management Software	2-6
Administrator Credentials	2-7
HA Redundancy Role	2-7
HA Redundancy States	2-8
Domain ID	2-8
Network Uplinks	2-8
VLANs	2-9
Management VLAN	2-9
Control VLAN	2-10
Setting up the Primary Cisco Nexus Virtual Services Appliance	2-10
Setting up the Secondary Cisco Nexus Virtual Services Appliance	2-16
Example for Network Uplink Configuration	2-17

Send document comments to nexus1k-docfeedback@cisco.com.

Verifying the Cisco Nexus Virtual Services Appliance Configuration 2-18
 Getting Started With Cisco Nexus Virtual Services Appliance 2-22
 Feature History for Software Installation 2-22

Cisco Nexus Virtual Services Appliance Software Upgrade 3-1

Information About In Service Software Upgrade 3-1
 Prerequisites 3-1
 Guidelines and Limitations 3-3
 Upgrading from Software Release 4.2(1)SP1(3) or Later 3-3
 Upgrade Example 3-5
 Feature History for Software Upgrade 3-12

Cisco Nexus Virtual Services Appliance Software Reinstallation 4-1

Reinstalling Cisco Nexus Virtual Services Appliance 4-1
 Information About Reinstalling the Software 4-1
 Guidelines and Limitations 4-1
 Reinstalling the Software 4-2
 Replacing a Cisco Nexus Virtual Services Appliance 4-2
 Feature History for Software Reinstallation 4-6



New and Changed Information

This section lists the new and changed information in this document by release, and where it is located.

Feature	Description	Changed in Release	Where Documented
IPv6 capability for management0 IP address	Enables you to specify management0 IPv6 address.	4.2(1)SP1(4a)	Chapter 2, “Cisco Nexus Virtual Services Appliance Software Installation”
Flexible Network Uplink	Enables you to specify flexible network uplink type.	4.2(1)SP1(4)	Chapter 2, “Cisco Nexus Virtual Services Appliance Software Installation”
Cisco Nexus 1010-X	Introduction of 1010-X	4.2(1)SP1(3)	Chapter 1, “Overview”
Software upgrade	Enables you to upgrade Cisco Nexus 1010.	4.2(1)SP1(2)	Chapter 3, “Cisco Nexus Virtual Services Appliance Software Upgrade”
Software reinstall	Enables you to reinstall Cisco Nexus 1010 software.	4.2(1)SP1(2)	Chapter 2, “Cisco Nexus Virtual Services Appliance Software Installation”

Send document comments to nexus1k-docfeedback@cisco.com.



Preface

This document describes how to install and upgrade Cisco Nexus Virtual Services Appliance .

This preface provides information about the *Cisco Nexus Virtual Services Appliance Software Installation and Upgrade Guide, Release 4.2(1) SP1(5.1)* in the following sections:

- [Audience, page v](#)
- [Recommended Reading, page v](#)
- [Organization, page vi](#)
- [Document Conventions, page vi](#)
- [Related Documentation, page vii](#)
- [Obtaining Documentation and Submitting a Service Request, page ix](#)

Audience

This document is for network administrators with knowledge of the Cisco Nexus 1000V and experience in the installation, upgrade, and management of Cisco Nexus 1000V VSMs.

Recommended Reading

Cisco recommends that you have read and are familiar with the following documentation:

- *Cisco Nexus Virtual Services Appliance Release Notes, Release 4.2(1)SP1(5.1)*
- *Cisco Nexus 1000V Software Installation and Upgrade Guide, Release 4.2(1)SV1(5.2)*
- *Cisco VN-Link: Virtualization-Aware Networking* white paper

Send document comments to nexus1k-docfeedback@cisco.com.

Organization

This document is organized as follows:

Chapter and Title	Description
Chapter 1, “Overview”	Provides an Overview on Cisco Nexus Virtual Services Appliance.
Chapter 2, “Cisco Nexus Virtual Services Appliance Software Installation”	Describes how to install Cisco Nexus Virtual Services Appliance.
Chapter 3, “Cisco Nexus Virtual Services Appliance Software Upgrade”	Describes how to upgrade Cisco Nexus Virtual Services Appliance.
Chapter 4, “Cisco Nexus Virtual Services Appliance Software Reinstallation”	Describes how to reinstall Cisco Nexus Virtual Services Appliance.

Document Conventions

This document uses the following conventions:



Note

Means reader *take note*. Notes contain helpful suggestions or references to material not covered in the manual.



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



Tip

Means *the following information will help you solve a problem*.

Send document comments to nexus1k-docfeedback@cisco.com.

Command descriptions use these conventions:

Convention	Description
boldface font	Commands and keywords are in boldface.
<i>italic font</i>	Arguments for which you supply values are in italics.
[]	Elements in square brackets are optional.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use these conventions:

screen font	Terminal sessions and information that the switch displays are in screen font.
boldface screen font	Information that you must enter is in boldface screen font.
<i>italic screen font</i>	Arguments for which you supply values are in italic screen font.
< >	Non-printing characters, such as passwords, are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or number sign (#) at the beginning of a line of code indicates a comment line.

Related Documentation

This section lists the documents used with the Cisco Nexus 1000 and available on [Cisco.com](http://www.cisco.com) at the following URL:

http://www.cisco.com/en/US/products/ps12752/tsd_products_support_series_home.html

General Information

Cisco Nexus 1000V Documentation Roadmap, Release 4.2(1)SV1(5.2)

Cisco Nexus 1000V Release Notes, Release 4.2(1)SV1(5.2)

Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(5.2)

Cisco Nexus Virtual Services Appliance Release Notes, Release 4.2(1)SP1(5.1a)

Install and Upgrade

Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.2)

Cisco Nexus Virtual Services Appliance Hardware Installation Guide

Cisco Nexus Virtual Services Appliance Software Installation and Upgrade Guide, Release 4.2(1)SP1(5.1a)

Send document comments to nexus1k-docfeedback@cisco.com.

Configuration Guides

Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.2(1)SVI(5.1)

Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SVI(5.1)

Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SVI(5.1)

Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SVI(5.1)

Cisco Nexus 1000V Network Segmentation Manager Configuration Guide, Release 4.2(1)SVI(5.1)

Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SVI(5.1)

Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.2(1)SVI(5.1)

Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SVI(5.1)

Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SVI(5.1)

Cisco Nexus 1000V VXLAN Configuration Guide, Release 4.2(1)SVI(5.1)

Cisco Nexus Virtual Services Appliance Software Configuration Guide, Release 4.2(1)SP1(5.1)

Programming Guide

Cisco Nexus 1000V XML API User Guide, Release 4.2(1)SVI(5.1)

Reference Guides

Cisco Nexus 1000V Command Reference, Release 4.2(1)SVI(5.1)

Cisco Nexus 1000V MIB Quick Reference

Cisco Nexus Virtual Services Appliance Command Reference, Release 4.2(1)SP1(5.1)

Troubleshooting and Alerts

Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SVI(5.1)

Cisco Nexus Virtual Services Appliance Troubleshooting Guide, Release 4.2(1)SP1(5.1)

Cisco Nexus 1000V Password Recovery Guide

Cisco Nexus 1000V Series and Cisco VSG NX-OS System Messages Reference

Cisco NX-OS Password Recovery Guide

Virtual Security Gateway Documentation

Cisco Virtual Security Gateway for Nexus 1000V Series Switch

Virtual Network Management Center

Cisco Virtual Network Management Center

Virtual Wide Area Application Services (vWAAS)

Cisco Virtual Wide Area Application Services (vWAAS)

ASA 1000V Cloud Firewall

Cisco ASA 1000V Cloud Firewall

Send document comments to nexus1k-docfeedback@cisco.com.

Network Analysis Module Documentation

Cisco Prime Network Analysis Module Software Documentation Guide, 5.1

Cisco Prime Network Analysis Module (NAM) for Nexus 1010 Installation and Configuration Guide, 5.1

Cisco Prime Network Analysis Module Command Reference Guide 5.1

Cisco Prime Network Analysis Module Software 5.1 Release Notes

Cisco Prime Network Analysis Module Software 5.1 User Guide

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Send document comments to nexus1k-docfeedback@cisco.com.



CHAPTER 1

Overview

This chapter describes the Cisco Nexus Virtual Services Appliance and includes the following sections:

- [Information About Cisco Nexus Virtual Services Appliance, page 1-1](#)
- [Cisco Integrated Management Controller, page 1-1](#)
- [Software Included, page 1-2](#)
- [Flow Chart: Installing and Configuring the Cisco Nexus Virtual Services Appliance, page 1-3](#)
- [Additional References, page 1-6](#)

Information About Cisco Nexus Virtual Services Appliance

The Cisco Nexus Virtual Services Appliance (VSA) product family includes Cisco Nexus 1010 and Cisco Nexus 1010-X. See the *Cisco Nexus Virtual Services Appliance Hardware Installation Guide* for more information.

The Cisco Nexus Virtual Services Appliance product family are networking appliances that can host up to six virtual service blades (VSBs) on Cisco Nexus 1010 and up to 10 VSBs on Cisco Nexus 1010-X.

Cisco Nexus Virtual Services Appliance product family supports VSBs like Cisco Nexus 1000V Virtual Supervisor Module (VSM), Network Analysis Module (NAM), and Virtual Security Gateway (VSG). The Cisco Nexus Virtual Services Appliance provides dedicated hardware for the Cisco Nexus 1000V VSM. VSMs that were hosted on VMware virtual machines can now be hosted on a Cisco Nexus Virtual Services Appliance. This allows you to install and manage the VSM like a standard Cisco switch. The services (VSM, VSG, or NAM) managed by the Cisco Nexus Virtual Services Appliance product family are called virtual service blades (VSBs).

See *Cisco Nexus Virtual Services Appliance Software Configuration Guide, Release 4.2(1)SP1(5.1)* for more information.

Cisco Integrated Management Controller

The Cisco Integrated Management Controller (CIMC) is a software interface included with the Cisco Nexus Virtual Services Appliance. CIMC allows you to configure serial over LAN (SoL) access and set up remote management in the event the device becomes unreachable. For more information about remote management, see the *Cisco Nexus Virtual Services Appliance Software Configuration Guide, Release 4.2(1)SP1(5.1)*.

[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

When installing the Cisco Nexus Virtual Services Appliance, you have the option to configure the CIMC interface. To configure the CIMC software while installing the Cisco Nexus Virtual Services Appliance, see the *Cisco Nexus Virtual Services Appliance Hardware Installation Guide*.

Supported PIDs for Cisco Nexus Virtual Services Appliance Product Family

This release supports the following hardware PIDs for the Cisco Nexus Virtual Services Appliance product family.

Cisco Nexus Virtual Services Appliance	Hardware PIDS
Cisco Nexus 1010	N1K-C1010
Cisco Nexus 1010-X	N1K-C1010-X

Software Included

The Cisco Nexus Virtual Services Appliance product family is shipped with the following software.

Software	Description	ISO filename in bootflash repository
Cisco Nexus 1010 or Cisco Nexus 1010-X ISO image	Image for the Cisco Nexus 1010 or Cisco Nexus 1010-X Manager virtual machine which manages the shelf and redundancy group configuration.	nexus-1010.4.2.1.SP1.5.1.iso ¹
Cisco Nexus 1000V VSM	Used to create a VSB for the Cisco Nexus 1000V VSM on the Cisco Nexus Virtual Services Appliance product family	nexus-1000v.4.2.1.SV1.5.1.iso ²
Cisco NAM VSB	Used to create a VSB for Cisco NAM on the Cisco Nexus Virtual Services Appliance product family	nam-app-x86_64.5-1-2.iso ²
Cisco VSG VSB	Used to create a VSB for Cisco VSG on the Cisco Nexus Virtual Services Appliance product family.	nexus-1000v.VSG1.3.1.iso
Cisco Integrated Management Controller (CIMC)	A software interface that allows you to manage the Cisco Nexus Virtual Services Appliance should it become unreachable.	N/A

1. In the event of disk corruption on the Cisco Nexus Virtual Services Appliance, the system can be brought up by copying the ISO image from a CD.
2. If it is necessary to update a VSB ISO file in bootflash, use the scp command to copy the new file version into the repository folder.

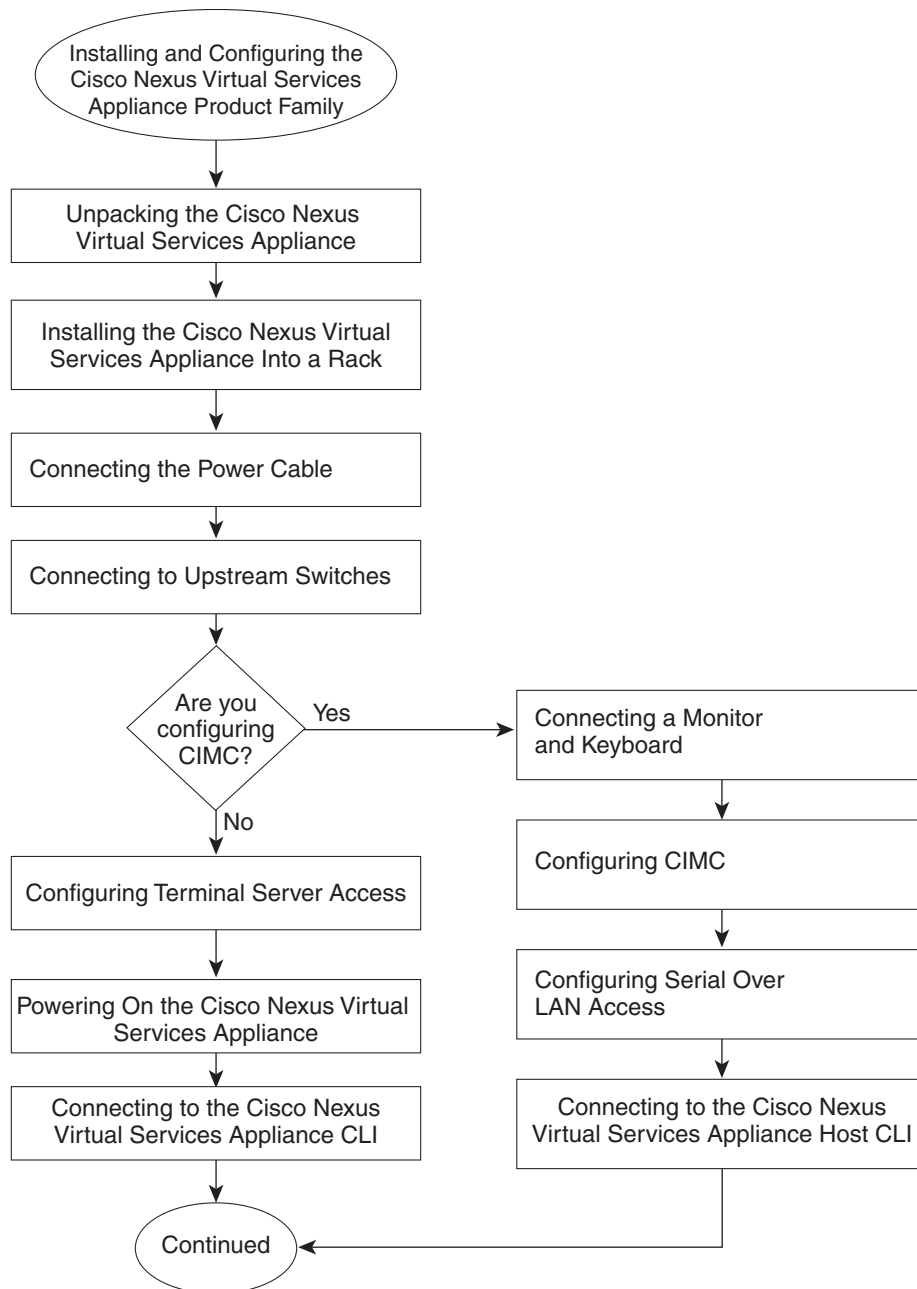
Send document comments to nexus1k-docfeedback@cisco.com.

Flow Chart: Installing and Configuring the Cisco Nexus Virtual Services Appliance

[Figure 1-1](#) and [Figure 1-2](#) show the basic steps for installing and configuring a Cisco Nexus Virtual Services Appliance. To install the Cisco Nexus Virtual Services Appliance hardware see the *Cisco Nexus Virtual Services Appliance Hardware Installation Guide*. To configure the Cisco Nexus Virtual Services Appliance product family see the *Cisco Nexus Virtual Services Appliance Software Configuration Guide, Release 4.2(1)SP1(5.1)*.

Send document comments to nexus1k-docfeedback@cisco.com.

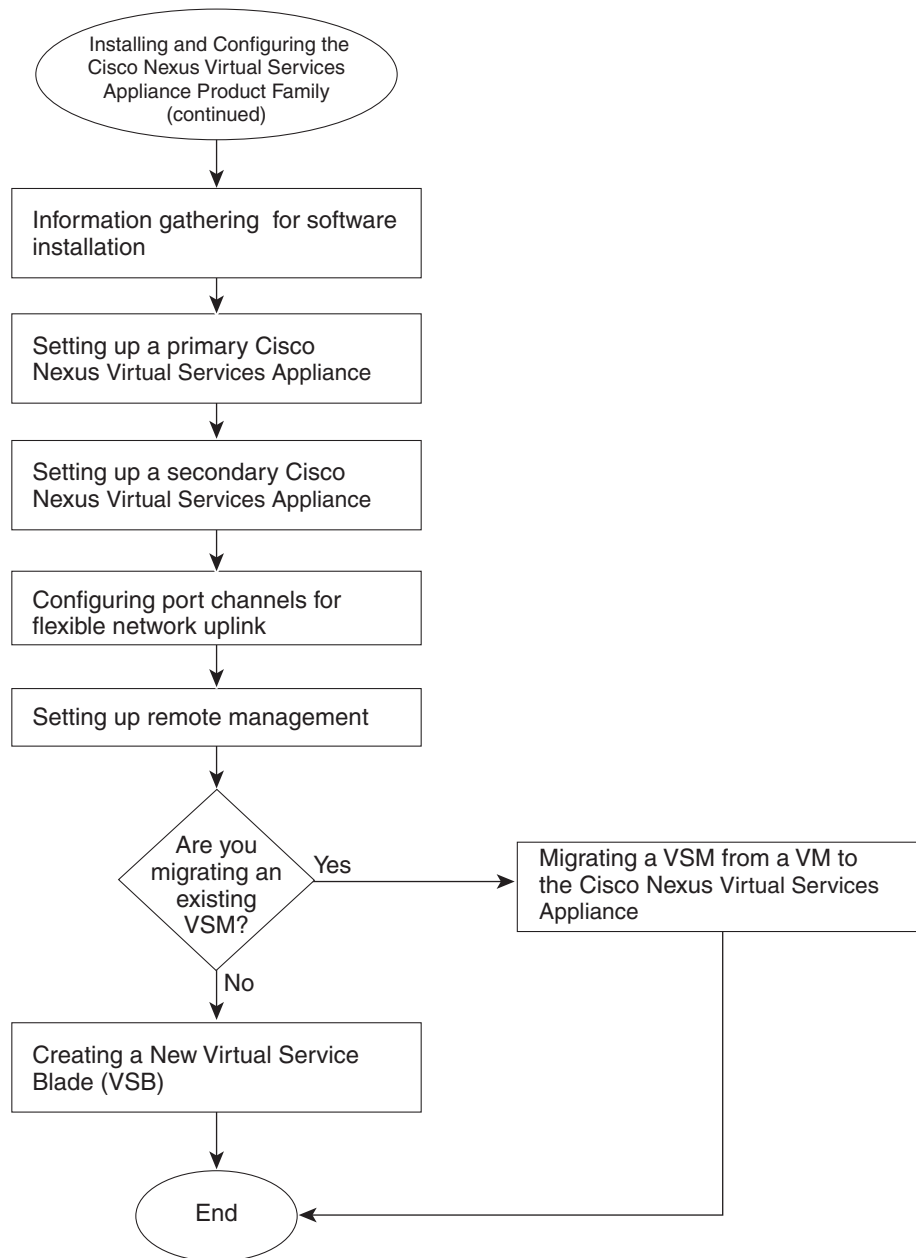
Figure 1-1 Flow Chart: Installing and Configuring the Cisco Nexus Virtual Services Appliance



282579

Send document comments to nexus1k-docfeedback@cisco.com.

Figure 1-2 ***Flow Chart: Installing and Configuring the Cisco Nexus Virtual Services Appliance (continued)***



282580

[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

Additional References

Related Topic	Document Title
Hardware installation	<i>Cisco Nexus Virtual Services Appliance Hardware Installation Guide</i>
Cisco Nexus Virtual Services Appliance software configuration	<i>Cisco Nexus Virtual Services Appliance Software Configuration Guide, Release 4.2(1)SP1(5.1)</i>
Cisco Nexus Virtual Services Appliance commands	<i>Cisco Nexus Virtual Services Appliance Command Reference, Release 4.2(1)SP1(5.1)</i>
CIMC management	<i>CIMC Firmware Management on UCS C-Series Servers</i>
Deployment	<i>Cisco Nexus Virtual Services Appliance Deployment Guide</i>



CHAPTER 2

Cisco Nexus Virtual Services Appliance Software Installation

This chapter describes how to install the Cisco Nexus Virtual Services Appliance software, and includes the following sections:

- [Information About Software Install, page 2-1](#)
- [Prerequisites, page 2-2](#)
- [Guidelines and Limitations, page 2-2](#)
- [Cisco Host Upgrade Utility Information, page 2-3](#)
- [Gathering Information About the Management Software, page 2-6](#)
- [Setting up the Primary Cisco Nexus Virtual Services Appliance, page 2-10](#)
- [Setting up the Secondary Cisco Nexus Virtual Services Appliance, page 2-16](#)
- [Example for Network Uplink Configuration, page 2-17](#)
- [Verifying the Cisco Nexus Virtual Services Appliance Configuration, page 2-18](#)
- [Getting Started With Cisco Nexus Virtual Services Appliance, page 2-22](#)
- [Feature History for Software Installation, page 2-22](#)



Note

For information about upgrading Cisco Nexus 1000V software on a VSB, see the *Cisco Nexus 1000V Software Installation and Upgrade Guide, Release 4.2(1)SV1(5.2)*.

For an overview of the Cisco Nexus Virtual Services Appliance product family and procedures for configuring the software after it is installed, see the *Cisco Nexus Virtual Services Appliance Software Configuration Guide, Release 4.2(1)SP1(5.1)*.

Information About Software Install

Cisco Nexus Virtual Services Appliance software is pre installed as an ISO image. Use this procedure to install the Cisco Nexus Virtual Services Appliance software. The installation involves the following steps:

-
- Step 1** Verify that you have the correct Cisco Integrated Management Controller (CIMC) software installed. See [Verifying the CIMC Software Version, page 2-4](#).

[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

- Step 2** Gather information about Management Software. See [Gathering Information About the Management Software, page 2-6](#).
- Step 3** Set up primary Cisco Nexus 1010 or Cisco Nexus 1010-X. See [Setting up the Primary Cisco Nexus Virtual Services Appliance, page 2-10](#)
- Step 4** Set up the secondary Cisco Nexus 1010 or Cisco Nexus 1010-X. See [Setting up the Secondary Cisco Nexus Virtual Services Appliance, page 2-16](#).

Prerequisites

Before installing Cisco Nexus Virtual Services Appliance Release 4.2(1)SP1(5.1), you must know or do the following:

- You must have the latest firmware release.



Note

It is a recommended Cisco best practice to upgrade the firmware using the **Cisco Host Upgrade Utility**. Failing to do so might result in network setup failure and/or system reboots. When using the HUU upgrade menu, choose the option to upgrade the CIMC, BIOS, and all other components of the hardware. For information on the Cisco Host Upgrade Utility, see [Cisco Host Upgrade Utility Information, page 2-3](#).

- You must have the following Cisco Integrated Management Controller (CIMC) software installed:
 - Version 1.4(3s)4 for the Cisco Nexus 1010 product family.
- Use the procedure described in [Verifying the CIMC Software Version, page 2-4](#), to verify that you have the appropriate CIMC version installed.



Note

- For firmware releases prior to version 1.4(3), the Cisco Host Upgrade Utility does not support Cisco Nexus 1010 and Cisco Nexus 1010-X. In such cases, use the Cisco Nexus Virtual Services Appliance CIMC GUI to manually update to CIMC version 1.4(3), and then use the Cisco Host Upgrade Utility to upgrade to firmware version 1.4(3s)4.
 - Upgrade to the latest CIMC version using the manual procedure in the [Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 1.4](#).
 - Upgrade the BIOS firmware version using the manual procedure in the [Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide](#).
- For firmware release 1.4(3) or higher, the Cisco UCS Host Upgrade Utility tool supports the Cisco Nexus Virtual Services Appliance. For more information see the [Cisco Host Upgrade Utility tool documentation](#).

Guidelines and Limitations

Follow these guidelines and limitations when setting up the Cisco Nexus Virtual Services Appliance product family:

- The domain ID must be unique within the VLAN.
- If other Cisco Nexus Virtual Services Appliances or Cisco Nexus 1000Vs are in the same VLAN, then the domain ID must also be unique across all of them.

Send document comments to nexus1k-docfeedback@cisco.com.

- When setting up the software, you configure the uplink type for your system. Once you configure an uplink type, the only way to modify it is to reload the software.
- The HA standalone role is not supported for the Cisco Nexus Virtual Services Appliance.
- Cisco Nexus Virtual Services Appliance is not supported in the non HA mode.
- It is a recommended Cisco best practice to configure a primary Cisco Nexus Virtual Services Appliance with a secondary backup. Although you can configure a primary Cisco Nexus Virtual Services Appliance without a secondary backup, this configuration in a production environment is not supported.
- It is recommended to configure the same domain ID, uplink type, control VLAN, management VLAN, control uplink, management uplink for both primary and secondary Cisco Nexus Virtual Services Appliances.
- The pairing of the Cisco Nexus Virtual Services Appliance must match the hardware platform. You cannot pair a Cisco Nexus 1010 with Cisco Nexus 1010-X.

Cisco Host Upgrade Utility Information

The Cisco Host Upgrade Utility (HUU) is a tool that you can use to upgrade the firmware on one or multiple Cisco UCS C-Series servers. The HUU detects the current version of the following components you have already installed, and guides you to upgrade them to the latest version:

- Cisco Integrated Management Controller (CIMC)
- System BIOS
- LAN on motherboard (LOM)
- RAID controllers
- Cisco UCS P81E Virtual Interface Card (VIC)
- Cisco UCS VIC 1225
- Cisco UCS VIC 1225-T
- Network adapters

You can obtain information about the minimum required version of the Cisco HUU, and how to download the HUU iso from the following sources:

- For Cisco Nexus 1010 product family, see the [Cisco Host Upgrade Utility Release 1.4\(3\) Quick Start Guide](#).

You must use the instructions provided in the HUU documentation to upgrade the firmware before you install the Cisco Nexus Virtual Services Appliance 4.2(1)SP1(5.1).



Caution

You must ensure to use the appropriate HUU version to upgrade your firmware.

[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

Verifying the CIMC Software Version

Use this procedure to verify that you have CIMC software Version 1.2.1(b) or higher installed on your Cisco Nexus Virtual Services Appliance.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You must have CIMC software Version 1.2.1(b) or higher installed.
- If CIMC software Version 1.2.1(b) or higher is installed, you will see the product ID N1K-C1010 on Cisco Nexus 1010 or the product ID N1K-C1010-X on Cisco Nexus 1010-X in the output of the **show hardware** command. This procedure includes steps for this verification.
- You are logged in to the Cisco Nexus Virtual Services Appliance from the CLI or a Web browser.

Step 1 From the Cisco Nexus Virtual Services Appliance do one of the following to display the product ID (PID):

- From the CLI, view the output of the **show hardware** command. Look in the Switch Hardware ID information for the PID.
- From a WEB browser, open the Server Summary window and view the server properties. See [Figure 2-1](#) for an example.

Example:

```
switch# show hardware
unset
Software
loader: version unset
kickstart: version unset
system: version unset
kickstart image file is: unset
kickstart compile time: unset [unset]
system image file is: unset
system compile time: unset [unset]

Hardware
cisco unset ("unset")
unset with unset unset of memory.
Processor Board ID unset

Device name: unset
bootflash: unset kB
Disk Storage capacity for VM virtual disks: 345945 MB
Number of physical 1Gbps ethernet ports: 6
Number of CPU Cores: 16
CPU Cores details:
model name : Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
model name : Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
model name : Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
model name : Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
model name : Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
model name : Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
model name : Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
model name : Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
model name : Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
model name : Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
model name : Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
model name : Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
model name : Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
model name : Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
model name : Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
```

Send document comments to nexus1k-docfeedback@cisco.com.

```
model name : Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
model name : Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
model name : Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
model name : Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz
```

```
Kernel uptime is unset day(s), unset hour(s), unset minute(s), unset second(s)
```

```
plugin
```

```
Core Plugin, Ethernet Plugin, Virtualization Plugin
```

```
-----
```

```
Switch hardware ID information
```

```
-----
```

```
Switch is booted up
```

```
Switch type is : Nexus 1110-S (Virtual Services Appliance) 2 slot Chassis
```

```
Model number is Nexus 1110-S
```

```
PID-VID-SN: N1K-C1110-S-2.0-1846886525134693056
```

```
-----
```

```
Chassis has 2 Module slots
```

```
-----
```

```
Module1 ok
```

```
Module type is : Cisco Virtual Services Appliance
```

```
0 submodules are present
```

```
Model number is Nexus 1110-S
```

```
H/W version is 2.0
```

```
UUID is 0F823778-D54A-4970-E999-2077C67F0133
```

```
Manufacture date is 02/22/2012
```

```
Serial number is
```

```
Module2 ok
```

```
Module type is : Cisco Virtual Services Appliance
```

```
0 submodules are present
```

```
Model number is Nexus 1110-S
```

```
H/W version is 2.0
```

```
UUID is 68143FE5-207B-4989-F297-0937998C9424
```

```
Manufacture date is 02/22/2012
```

```
Serial number is QCI1410A4LP
```

Send document comments to nexus1k-docfeedback@cisco.com.

Figure 2-1 CIMC Window with Product ID (PID)



Step 2 Do one of the following:

- If the PID displayed is N1K-C1010 on Cisco Nexus 1010 or N1K-C1010-X on Cisco Nexus 1010-X, you can proceed with the install or upgrade to Cisco Nexus Virtual Services Appliance Release 4.2(1)SP1(5.1).
- If the PID displayed is not N1K-C1010 on Cisco Nexus 1010 or N1K-C1010-X on Cisco Nexus 1010-X, do not install or upgrade to Release 4.2(1)SP1(5.1). Instead you must replace the Cisco Nexus Virtual Services Appliance using the RMA process. See [Replacing a Cisco Nexus Virtual Services Appliance](#), page 4-2.

Gathering Information About the Management Software

Before you begin the installation, you will need the following information for your Cisco Nexus Virtual Services Appliance:

- [Administrator Credentials](#), page 2-7
- [HA Redundancy Role](#), page 2-7
- [HA Redundancy States](#), page 2-8
- [Domain ID](#), page 2-8
- [Network Uplinks](#), page 2-8
- [VLANs](#), page 2-9

Send document comments to nexus1k-docfeedback@cisco.com.

Administrator Credentials

When you set up the system software, you are required to create an administrator password. [Table 2-1](#) lists password strength guidelines:

Table 2-1 Guidelines for strong passwords

Strong passwords have:	Strong passwords do NOT have:
<ul style="list-style-type: none"> • At least eight characters • Uppercase letters • Lowercase letters • Numbers • Special characters 	<ul style="list-style-type: none"> • Consecutive characters, such as “abcd” • Repeating characters, such as “aaabbb” • Dictionary words • Proper names

HA Redundancy Role

The Cisco Nexus Virtual Services Appliance product family is provided in redundant pairs for high availability. When setting up the device, you configure a high availability role—primary or secondary. [Table 2-2](#) describes these roles.



Note

The HA standalone role is not supported for the Cisco Nexus Virtual Services Appliance product family. Cisco Nexus Virtual Services Appliance is not supported in a non HA mode.

Table 2-2 HA Redundancy Roles

Role	Description
Primary	<ul style="list-style-type: none"> • The primary role coordinates the active/standby redundancy state with the secondary Cisco Nexus Virtual Services Appliance. • The primary role takes precedence during bootup when negotiating active/standby redundancy state. That is, if the secondary Cisco Nexus Virtual Services Appliance is not in the active state at bootup, the primary Cisco Nexus Virtual Services Appliance takes the active redundancy state. • You assign the primary role to the first Cisco Nexus Virtual Services Appliance that you install in a dual system.
Secondary	<ul style="list-style-type: none"> • The secondary role coordinates the active/standby state with the primary Cisco Nexus Virtual Services Appliance. • You assign the secondary role to the second Cisco Nexus Virtual Services Appliance that you install in a dual system.

[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

HA Redundancy States

Table 2-3 describes the HA redundancy states.

Table 2-3 HA Redundancy States

Redundancy State	Description
Active	<p>Controls the system and is visible to the outside world.</p> <p>The active system is remotely accessed through the network after initial setup.</p> <p>The user interface for managing the Cisco Nexus Virtual Services Appliance is only available through the active system.</p>
Standby	<p>Synchronizes its configuration with that of the active Cisco Nexus Virtual Services Appliance so that it is continuously ready to take over in case of a failure or manual switchover.</p> <p>You cannot use Telnet or Secure Shell (SSH) protocols to communicate with the standby Cisco Nexus Virtual Services Appliance.</p> <p>The standby Cisco Nexus Virtual Services Appliance is not network addressable and is accessed through the serial port.</p> <p>The user interface for managing the Cisco Nexus Virtual Services Appliance is not available through the standby system.</p>

Domain ID

The primary and secondary Cisco Nexus Virtual Services Appliances use the domain ID to identify each other. The Cisco Nexus Virtual Services Appliances must be in the same switching domain, and share the same management IP address.

Network Uplinks

Cisco Nexus Virtual Services Appliance product family supports two types of network uplink configurations to connect to the network.

- **Flexible Network Uplink:** Flexible network configuration offers complete flexibility to connect the Cisco Nexus Virtual Services Appliance product family to the network and allows you to achieve a maximum of six uplinks.
- **Static Network Uplink :** In a static network configuration, the Cisco Nexus Virtual Services Appliance product family is connected to the network using four fixed network uplink configurations. See [Table 2-4 Network Uplink Types, page 2-9](#).

As a result you can connect your system to the network using one of the following five supported uplink types.

- One uplink
- Two uplinks with common management and control traffic
- Two uplinks with common control and data traffic
- Three uplinks

Send document comments to nexus1k-docfeedback@cisco.com.

- Flexible network uplink



Note Once you configure an uplink type, the only way to modify it is to reload the software.

See the *Cisco Nexus Virtual Services Appliance Software Configuration Guide, Release 4.2(1)SP1(5.1)* for more information about network uplink types.

During the installation of Cisco Nexus Virtual Services Appliance product family you can setup the flexible network uplink type or the static network uplink type. If you modify the uplink type, a reload is required each time the uplink type is modified for it to take effect.

See the *Cisco Nexus Virtual Services Appliance Software Configuration Guide, Release 4.2(1)SP1(5.1)* for information about migrating the network uplink types.

Table 2-4 shows the four supported network uplink types and the ports that carry each type of VLAN traffic.

Table 2-4 Network Uplink Types

Uplink type	Management VLAN	Control VLAN	Data VLAN
1	ports 1 and 2	ports 1 and 2	ports 1 and 2
2	ports 1 and 2	ports 1 and 2	ports 3-6
3	ports 1-2	ports 3-6	ports 3-6
4	ports 1-2	ports 3-4	ports 5-6
Flexible	There is no traffic segregation based on traffic class		

VLANs

Control, and management VLANs are used by the Cisco Nexus Virtual Services Appliance product family for management and communication with its virtual service blades. These VLANs are added as a part of the initial setup of the management software. Control and packet VLANs are also added to each virtual service blade when it is created. The management VLAN is inherited from the Cisco Nexus Virtual Services Appliance product family by each virtual service blade.

If you modify a control, packet, or management VLAN on the Cisco Nexus Virtual Services Appliance product family, the change is effective immediately. A reload is required to effect the change of control and management VLAN on Cisco Nexus Virtual Services Appliance. However, for service continuity, you must configure the same control and packet VLANs on the hosted VSMs. Otherwise the Cisco Nexus Virtual Services Appliance loses communication with its VSMs.

This section includes the following additional topics:

- [Management VLAN, page 2-9](#)
- [Control VLAN, page 2-10](#)

Management VLAN

The management VLAN is the VLAN that forwards traffic for the management port of the Cisco Nexus Virtual Services Appliance. If your virtual service blade uses the management class of traffic, it inherits the management VLAN from the Cisco Nexus Virtual Services Appliance.

The management VLAN is used by the outside world to reach the Cisco Nexus Virtual Services Appliance management 0 interface.

Send document comments to nexus1k-docfeedback@cisco.com.

The Cisco Nexus Virtual Services Appliance and its hosted Cisco Nexus 1000 VSMs share the same management VLAN in static topology. Unlike the control and packet VLANs which are set when a VSB is created, the management VLAN is inherited. In a static topology, the management VLAN on a VSB cannot be changed. Since the management VLAN is inherited from the Cisco Nexus Virtual Services Appliance, if you change management VLAN for Cisco Nexus Virtual Services Appliance, then the change is applied to both the Cisco Nexus Virtual Services Appliance and all of its hosted Cisco Nexus 1000 VSMs in next reload.

However, this constraint does not exist in flexible topology and the management VLAN of a VSB can be different from the Cisco Nexus Virtual Services Appliance host.

Control VLAN

The control VLAN is a Layer 2 interface used for communication between the redundant Cisco Nexus Virtual Services Appliances. This interface handles low-level control packets such as heartbeats as well as any configuration data that needs to be exchanged between the Cisco Nexus 1010s.

Setting up the Primary Cisco Nexus Virtual Services Appliance

You can use this procedure to set up the management software for the following:

- The primary Cisco Nexus Virtual Services Appliance in a redundant HA pair

It is a recommended Cisco best practice to configure a primary Cisco Nexus Virtual Services Appliance with a secondary backup. Although you can configure a primary Cisco Nexus Virtual Services Appliance without a secondary backup, this configuration in a production environment is not supported.

BEFORE YOU BEGIN

- You have the following information available for this Cisco Nexus Virtual Services Appliance:
 - Administrator password
 - HA role (primary or secondary)
If you do not specify an HA role, then the role is configured as primary.
 - Network uplink type
 - Control VLAN ID
 - Domain ID
 - Management VLAN ID
 - Management 0 IP address
This is the IP address of the management interface that appears as the mgmt0 port on the appliance.
 - Default gateway IP address
 - SSH service key type and number of key bits

DETAILED STEPS

-
- Step 1** Use one of the following methods to log in to the Cisco Nexus Virtual Services Appliance.
The setup wizard starts automatically.

Send document comments to nexus1k-docfeedback@cisco.com.

- Login from a terminal server:

```

Example:
telnet 172.25.182.99 2005
Trying 172.25.182.99...
Connected to 172.25.182.99.
Escape character is '^]'
switch#

---- System Admin Account Setup ----
Enter the password for "admin":
Confirm the password for "admin":

```

- Login from a serial over LAN connection through CIMC:

```

Example:
ssh admin@172.25.182.230
admin@172.25.182.230's password:
switch# connect host
CISCO Serial Over LAN:
Close Network Connection to Exit

---- System Admin Account Setup ----
Enter the password for "admin":
Confirm the password for "admin":

```

- Step 2** When asked, enter and confirm the Administrator password.

```

Example:
---- System Admin Account Setup ----
Enter the password for "admin":
Confirm the password for "admin":

```

- Step 3** When asked, enter the HA role. If you do not specify a role, then primary is assigned.

```

Example:
Enter HA role[primary/secondary]: primary

```



Note The HA standalone role is not supported for the Cisco Nexus Virtual Services Appliance product family. Cisco Nexus Virtual Services Appliance is not supported in a non HA mode

- Step 4** When asked, enter the uplink type. To specify static network uplink, enter a value from 1-4. To specify flexible network uplink, enter the value 5.



Note Once you configure an uplink type, the only way to modify it is to reload the software.

```

Example:
Enter network-uplink type <1-5>:
  1. Ports 1-2 carry all management, control and data vlans
  2. Ports 1-2 management and control, ports 3-6 data
  3. Ports 1-2 management, ports 3-6 control and data
  4. Ports 1-2 management, ports 3-4 control, ports 5-6 data
  5. Flexible
5

```

- Step 5** When asked, enter the VLAN ID for the control VLAN.

```

Example:
Enter control vlan <1-3967, 4048-4093>: 1481

```

Send document comments to nexus1k-docfeedback@cisco.com.

Step 6 When asked, enter control uplink.

Example:

```
Enter control uplink <1-6>: 1
```

Step 7 When asked, enter the domain ID.

Example:

```
Enter the domain id<1-4095>: 121
```

Step 8 When asked, enter the VLAN ID for the management VLAN.

Example:

```
Enter management vlan<1-3967,4048-4093>: 1490
```

Step 9 When asked, enter management uplink.

Example:

```
Enter management uplink <1-6>: 1
```

Step 10 When you have completed this process, the Cisco Nexus Virtual Services Appliance software saves the configuration and automatically reboots to configure the network uplinks.

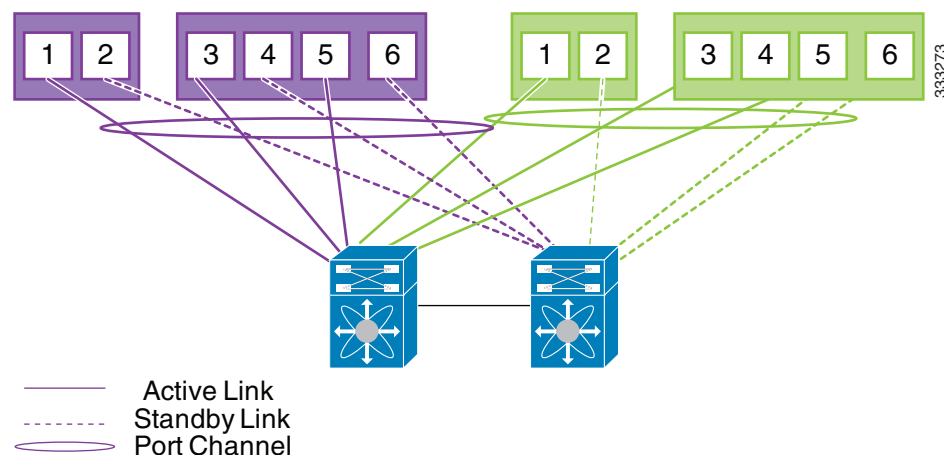
The new configuration is saved into nonvolatile storage, after which the running and the startup copies of the configuration are identical.

```
Saving boot configuration. Please wait...
```

```
[#####] 100%
System is going to reboot to configure network uplinks
```

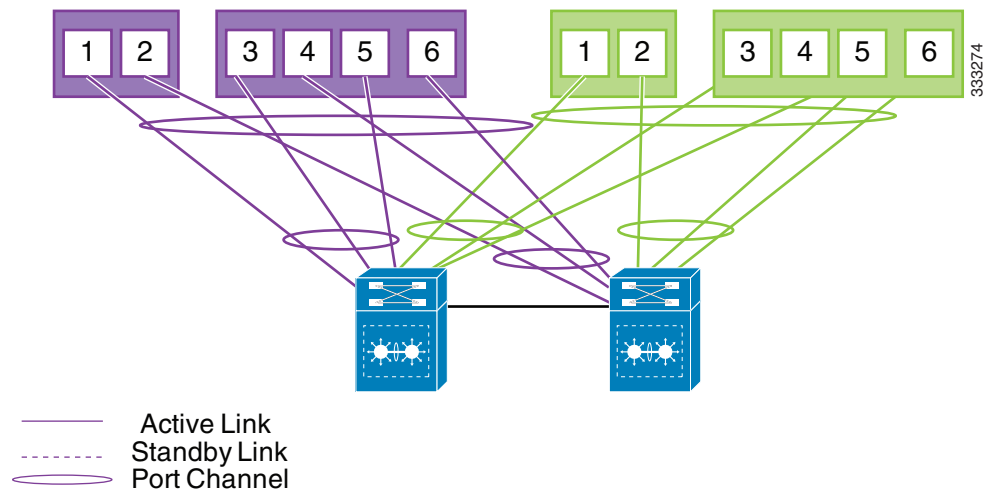
After reboot, the default static or flexible topology will be configured. See [Figure 2-2](#) for default flexible network uplink configuration. For more information, see the *Cisco Nexus Virtual Services Appliance Software Configuration Guide, Release 4.2(1)SP1(5.1)*.

Figure 2-2 Default Flexible Network Uplink Configuration without vPC /VSS



Send document comments to nexus1k-docfeedback@cisco.com.

Figure 2-3 Default Flexible Network Uplink Configuration with vPC /VSS



Step 11 When asked if you want to enter the basic configuration dialog, respond **yes**.

Example:

Would you like to enter the basic configuration dialog (yes/no): **yes**

---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

*Note: setup is mainly used for configuring the system initially, when no configuration is present. So setup always assumes system defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip the remaining dialogs.

Step 12 When asked to create another Login account, answer **no**.

Example:

Create another login account (yes/no) [n]: **no**

Step 13 When asked to configure a read-only SNMP community string, answer **no**.

Example:

Configure read-only SNMP community string (yes/no) [n]: **no**

Step 14 When asked to configure a read-write SNMP community string, answer **no**.

Example:

Configure read-write SNMP community string (yes/no) [n]:

Step 15 Enter a name for the appliance.

Example:

Enter the VSA name : N1010

Step 16 When asked to configure out-of-band management, answer **yes** and then enter the management 0 IPv4/IPv6 address.

This is the IP address of the management interface that appears as the mgmt0 port on the appliance.

Send document comments to nexus1k-docfeedback@cisco.com.

Example:

```
Continue with Out-of-band (mgmt0) management configuration? [yes/no] [y]: yes
Mgmt0 IP address type V4/V6? (V4): V4
Mgmt0 IPv4 address: 45.45.45.3
Mgmt0 IPv4 netmask :255.255.255.0
```

Step 17 When asked to configure the default gateway, answer **yes**.

Example:

```
Configure the default-gateway: (yes/no) [y]: yes
IPv4 address of the default gateway: 45.45.45.1
```

Step 18 When asked to configure advanced IP options, answer **no**.

Example:

```
Configure Advanced IP options (yes/no)? [n]: no
```

Step 19 When asked to enable the Telnet service, answer **no**.

Example:

```
Enable the telnet service? (yes/no) [y]: no
```

Step 20 When asked to enable the SSH service, answer **yes** and then enter the key type and number of key bits.

Example:

```
Enable the ssh service? (yes/no) [y]: yes
Type of ssh key you would like to generate (dsa/rsa) : rsa
Number of key bits <768-2048> : 1024
```

Step 21 When asked to enable the HTTP server, answer **yes**

Step 22 When asked to configure the NTP server, answer **no**.

The configuration is summarized.

Example:

```
Configure NTP server? (yes/no) [n]: no
The following configuration will be applied:
interface mgmt0
 ip address 45.45.45.3 255.255.255.0
 no shutdown
 vrf context management
 ip route 0.0.0.0/0 45.45.45.1
 no telnet server enable
 ssh key rsa 1024 force
 ssh server enable
 feature http-server
```

Step 23 Do one of the following:

- If you do not want to edit the configuration answer **no** and continue with the next step.
- If you want to edit the configuration, answer **yes** and return to [Step 12](#) to revisit each command.

Example:

```
Would you like to edit the configuration? (yes/no) [n]:no
```

Step 24 When asked to use and save this configuration, answer **yes**.

**Caution**

If you do not save the configuration now, then none of your changes are part of the configuration the next time the switch is rebooted. Enter **yes** to save the new configuration. This ensures that the kickstart and system images are also automatically configured.

Send document comments to nexus1k-docfeedback@cisco.com.

Example:

```
Use this configuration and save it? (yes/no) [y]: yes
[#####] 100%
```

The new configuration is saved into nonvolatile storage, after which the running and the startup copies of the configuration are identical.



Note You can use the setup routine to update the configuration done in [Step 12](#) through [Step 24](#) at any time by entering the **setup** command in EXEC mode. Once setup begins, press Enter to skip a command. Use ctrl-c to skip the remaining commands.

Step 25 You have completed this procedure. You can verify the configuration using the following command:

show running configuration

```
N1010# sh run

!Command: show running-config
!Time: Thu Feb 27 02:57:25 2014

version 4.2(1)SP1(5.1)
no feature telnet

username admin password 5 $1$BzSSk6qR$m.FMEvkOXzutuLwrmVeUe/ role network-admin

banner motd #Cisco VSA#

ip domain-lookup
ip domain-lookup
hostname N1010
snmp-server user admin network-admin auth md5 0xb64ad6879970f0e57600c443287a79f0
priv 0xb64ad6879970f0e57600c443287a79f0 localizedkey

vrf context management
 ip route 0.0.0.0/0 45.45.45.1
vlan 1,1481,1490
port-channel load-balance ethernet source-mac
port-profile default max-ports 32

vdc N1010 id 1
 limit-resource vlan minimum 16 maximum 2049
 limit-resource monitor-session minimum 0 maximum 2
 limit-resource vrf minimum 16 maximum 8192
 limit-resource port-channel minimum 0 maximum 768
 limit-resource u4route-mem minimum 32 maximum 32
 limit-resource u6route-mem minimum 16 maximum 16
 limit-resource m4route-mem minimum 58 maximum 58
 limit-resource m6route-mem minimum 8 maximum 8
network-uplink type 5
interface GigabitEthernet1
interface GigabitEthernet2
interface GigabitEthernet3
interface GigabitEthernet4
interface GigabitEthernet5
interface GigabitEthernet6
svs-domain
 control uplink GigabitEthernet1
 management uplink GigabitEthernet1

interface mgmt0
 ip address 45.45.45.3/24
```

Send document comments to nexus1k-docfeedback@cisco.com.

```
interface control0
line console
svs-domain
  domain id 121
  control vlan 1481
  management vlan 1490
  svs mode L2
N1010
```

Setting up the Secondary Cisco Nexus Virtual Services Appliance

You can use this procedure to set up the management software for the secondary Cisco Nexus Virtual Services Appliance in a redundant pair.

It is recommended to configure the same domain ID, uplink type, control VLAN, management VLAN, control uplink, management uplink for both primary and secondary Cisco Nexus Virtual Services Appliances.

DETAILED STEPS

Step 1 When asked, enter and confirm the Administrator password.

Example:

```
---- System Admin Account Setup ----
Enter the password for "admin":
Confirm the password for "admin":
```

Step 2 When asked, enter the HA role.

Example:

```
Enter HA role[primary/secondary]: secondary
```

Step 3 When asked, enter the uplink type.



Note Once you configure an uplink type, the only way to modify it is to reload the software.

Example:

```
Enter network-uplink type <1-5>:
  1. Ports 1-2 carry all management, control and data vlans
  2. Ports 1-2 management and control, ports 3-6 data
  3. Ports 1-2 management, ports 3-6 control and data
  4. Ports 1-2 management, ports 3-4 control, ports 5-6 data
  5. Flexible
5
```

Step 4 When asked, enter the VLAN ID for the control VLAN.

Example:

```
Enter control vlan <1-3967, 4048-4093>: 347
```

Send document comments to nexus1k-docfeedback@cisco.com.

Step 5 When asked, enter control uplink type.

Example:

```
Enter control uplink <1-6>: 1
```

Step 6 When asked, enter the domain ID.

Example:

```
Enter the domain id<1-4095>: 3477
```

Step 7 When asked, enter the VLAN ID for the management VLAN.

Example:

```
Enter management vlan<1-3967,4048-4093>: 180
```

Step 8 When asked, enter management uplink type.

Example:

```
Enter management uplink <1-6>: 2
```

The following things occur on the switch:

- The new configuration is saved into nonvolatile storage, after which the running and the startup copies of the configuration are identical.
- The system reboots to configure the network uplinks.
- The system restarts and synchronizes its configuration with the primary Cisco Nexus 1000V.

Example:

```
Saving boot configuration. Please wait...
```

```
[#####] 100%
```

```
System is going to reboot to configure network uplinks
HA mode set to secondary. Rebooting now...
```

Step 9 You have completed this procedure. You can verify the configuration using the following command:
show running configuration.

Example for Network Uplink Configuration

The following example shows how to configure flexible network uplink configuration during installation:

```
---- System Admin Account Setup ----
Enter the password for "admin":
Confirm the password for "admin":
Enter HA role[primary/secondary]: secondary

-
Enter network-uplink type <1-5>:
1. Ports 1-2 carry all management, control and data vlans
2. Ports 1-2 management and control, ports 3-6 data
3. Ports 1-2 management, ports 3-6 control and data
4. Ports 1-2 management, ports 3-4 control, ports 5-6 data
5. Flexible
5

-
Enter control vlan <1-3967, 4048-4093>: 347
Enter control uplink <1-6>: 1
```

Send document comments to nexus1k-docfeedback@cisco.com.

```

- Enter the domain id<1-4095>: 3477
- Enter management vlan <1-3967, 4048-4093>: 180
  Enter management uplink <1-6>: 2
- Saving boot configuration. Please wait...
[#####] 100%
  System is going to reboot to configure network uplinks

```

The following example shows how to configure static network uplink configuration during installation:

```

---- System Admin Account Setup ----
  Enter the password for "admin":
  Confirm the password for "admin":
  Enter HA role[primary/secondary]: secondary
- Enter network-uplink type <1-5>:
  1. Ports 1-2 carry all management, control and data vlans
  2. Ports 1-2 management and control, ports 3-6 data
  3. Ports 1-2 management, ports 3-6 control and data
  4. Ports 1-2 management, ports 3-4 control, ports 5-6 data
  5. Flexible
1
- Enter control vlan <1-3967, 4048-4093>: 300
- Enter the domain id<1-4095>: 300
- Enter management vlan <1-3967, 4048-4093>: 233
- Saving boot configuration. Please wait...
[#####] 100%
  System is going to reboot to configure network uplinks

```

Verifying the Cisco Nexus Virtual Services Appliance Configuration

To verify the Cisco Nexus Virtual Services Appliance configuration, use the following commands:

Command	Purpose
show running-configuration	Displays the Cisco Nexus Virtual Services Appliance running configuration. See Example 2-1 on page 2-19 .
show system redundancy status	Displays the redundancy state (active or standby) and the redundancy role (primary or secondary) for the Cisco Nexus Virtual Services Appliances. See Example 2-2 on page 2-21 .

Send document comments to nexus1k-docfeedback@cisco.com.

Command	Purpose
show svcs domain	Displays the domain information for the Cisco Nexus Virtual Services Appliance: See Example 2-3 on page 2-21 .
show network cdp neighbors	Displays uplink connectivity for the active or standby Cisco Nexus Virtual Services Appliance. See Example 2-4 on page 2-21 .

Example 2-1 Setup Configuration

This example shows how to display and verify the Cisco Nexus Virtual Services Appliance setup configuration:

show running-config

```
!Command: show running-config
!Time: Mon Sep 10 21:31:34 2012

version 4.2(1)SP1(5.1)
feature telnet

username admin password 5 $1$8oEF.umL$mRRZTm3.sWL2ED5KZydz61 role network-admin

banner motd #Cisco VSA#

ip domain-lookup
ip domain-lookup
hostname N1110-S
snmp-server user admin network-admin auth md5 0xb64ad6879970f0e57600c443287a79f0 priv
0xb64ad6879970f0e57600c443287a79f0 localizedkey
snmp-server community public group network-admin

vrf context management
ip route 0.0.0.0/0 10.78.109.97
vlan 1,1352,1360
port-channel load-balance ethernet source-mac
port-profile default max-ports 32

vdc N1110-S id 1
limit-resource vlan minimum 16 maximum 2049
limit-resource monitor-session minimum 0 maximum 2
limit-resource vrf minimum 16 maximum 8192
limit-resource port-channel minimum 0 maximum 768
limit-resource u4route-mem minimum 32 maximum 32
limit-resource u6route-mem minimum 16 maximum 16
limit-resource m4route-mem minimum 58 maximum 58
limit-resource m6route-mem minimum 8 maximum 8
network-uplink type 4
interface GigabitEthernet1
interface GigabitEthernet2
interface GigabitEthernet3
interface GigabitEthernet4
interface GigabitEthernet5
interface GigabitEthernet6
interface PortChannel1
interface PortChannel2
interface PortChannel3
virtual-service-blade VSM1
virtual-service-blade-type name VSM-1.1
interface control vlan 1361
```

Send document comments to nexus1k-docfeedback@cisco.com.

```

interface packet vlan 1362
  ramsize 2048
  disksize 3
  numcpu 1
  cookie 1555871292
  no shutdown
interface VsbEthernet1/1
interface VsbEthernet1/2
interface VsbEthernet1/3
virtual-service-blade NAMC-1
virtual-service-blade-type name NAM-1.1
interface data vlan 1352
  ramsize 2048
  disksize 53
  numcpu 2
  cookie 753232953
  no shutdown secondary
interface VsbEthernet2/1
virtual-service-blade DCNM61
virtual-service-blade-type name DCNM-VSB-6.1
interface eth1 vlan 0
  ramsize 8192
  disksize 80
  numcpu 2
  cookie 969732378
  no shutdown primary
interface VsbEthernet3/1
virtual-service-blade VSG12
virtual-service-blade-type name VSG-1.2
interface data vlan 1365
interface ha vlan 1364
  ramsize 2048
  disksize 3
  numcpu 1
  cookie 2051820775
  no shutdown primary
  no shutdown secondary
interface VsbEthernet4/1
interface VsbEthernet4/2
interface VsbEthernet4/3
virtual-service-blade VSM-OVA
virtual-service-blade-type name VSM-1.2
interface control vlan 1364
interface packet vlan 1366
  ramsize 2048
  disksize 3
  numcpu 1
  cookie 448734513
  no shutdown primary
  no shutdown secondary
interface VsbEthernet5/1
interface VsbEthernet5/2
interface VsbEthernet5/3
virtual-service-blade VSG-OVA
virtual-service-blade-type name VSG-1.2
interface data vlan 1356
interface ha vlan 1355
  ramsize 2048
  disksize 3
  numcpu 1
  cookie 2105102293
  no shutdown
interface VsbEthernet6/1
interface VsbEthernet6/2

```

Send document comments to nexus1k-docfeedback@cisco.com.

```
interface VsbEthernet6/3

interface mgmt0
ip address 10.78.109.100/28

interface control0
line console
boot kickstart bootflash:/nexus-1010-kickstart-mz.4.2.1.SP1.5.1.bin
boot system bootflash:/nexus-1010-mz.4.2.1.SP1.5.1.bin
boot kickstart bootflash:/nexus-1010-kickstart-mz.4.2.1.SP1.5.1.bin
boot system bootflash:/nexus-1010-mz.4.2.1.SP1.5.1.bin
svs-domain
domain id 2222
control vlan 1360
management vlan 1352
svs mode L2
```

Example 2-2 Redundancy Status

```
switch# show system redundancy status
Redundancy role
-----
      administrative:  primary
      operational:    primary
Redundancy mode
-----
      administrative:  HA
      operational:    None
This supervisor (sup-1)
-----
      Redundancy state:  Active
      Supervisor state:  Active
      Internal state:    Active with no standby
Other supervisor (sup-2)
-----
      Redundancy state:  Not present
-----
switch#
```

Example 2-3 Domain

```
switch# show svs domain
SVS domain config:
  Domain id:      3555
  Control vlan:  305
  Management vlan: 233
  L2/L3 Control mode: L2
  L3 control interface: NA
  Status: Config not pushed to VC.
switch#
```

Example 2-4 CDP neighbors (standby)

```
switch# show network cdp neighbors
...
Device-ID           Local Intrfce Hldtme Capability Platform      Port ID
-----
sfish-cat3k-K5-stack2 eth2           166      R T B S I r cisco WS-C375 GigabitEthernet1/0/23
switch#
```

[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

Getting Started With Cisco Nexus Virtual Services Appliance

After you complete the software installation, you can configure the Cisco Nexus Virtual Services Appliance product family. See the *Cisco Nexus Virtual Services Appliance Software Configuration Guide, Release 4.2(1)SP1(5.1)* for more information

The following are the basic steps in the software configuration process.

-
- Step 1** Configuring port channels for flexible network uplink. Use this procedure to configure port channels after you set up the flexible network uplink type.
- Step 2** Setting up remote management. Use this procedure to set up remote management in your startup configuration for use in recovering an unreachable Cisco Nexus Virtual Services Appliance.
- Step 3** Do one of the following to add a service blades to the new Cisco Nexus Virtual Services Appliance :
- Create a new virtual service blade.
 - Migrate an existing VSM from a VM to the Cisco Nexus Virtual Services Appliance.
-

Feature History for Software Installation

This section provides the software installation and upgrade release history.

Feature Name	Releases	Feature Information
Flexible Network Uplink	4.2(1)SP1(4)	This feature was introduced.
Cisco Nexus 1010-X	4.2(1)SP1(3)	This hardware was introduced.
Software upgrade	4.2(1)SP1(2)	This feature was introduced.



CHAPTER 3

Cisco Nexus Virtual Services Appliance Software Upgrade

This chapter describes how to upgrade Cisco Nexus Virtual Services Appliance product family to the new version and includes the following sections:

- [Prerequisites, page 3-1](#)
- [Upgrading from Software Release 4.2\(1\)SP1\(3\) or Later, page 3-3](#)
- [Upgrade Example, page 3-5](#)

Information About In Service Software Upgrade

The Cisco Nexus Virtual Services Appliance upgrade is a hitless in-service software upgrade (ISSU). When you upgrade the software, the operational data is retained without loss of persistent information. The availability of VSBs will not be affected during the upgrade process.

Once the command to upgrade is issued, the whole upgrade procedure is automated. The upgrade process takes time and follows the following sequence:

- First the ISO image components are extracted, verified and synchronized to the standby Cisco Nexus Virtual Services Appliance.
- The standby Cisco Nexus Virtual Services Appliance is upgraded first.
- The VSBS on the standby are restarted.
- The upgrade of the active is initiated.
- Once the upgrade of active and standby is complete both will form a HA pair running the upgraded software.

Finally, the ISSU is complete when both Cisco Nexus Virtual Services Appliances form an HA pair with the new software version.

Prerequisites

Before beginning this procedures in this section you must know or do the following:

- You have verified that you have the following product ID (PID), using the [Verifying the CIMC Software Version, page 2-4](#).
 - N1K-C1010 on Cisco Nexus 1010

Send document comments to nexus1k-docfeedback@cisco.com.

- N1K-C1010-X on Cisco Nexus 1010-X



Caution

You cannot install or upgrade to Release 4.2(1)SP1(5.1) unless your Cisco Nexus 1010 has the product ID (PID) N1K-C1010 or your Cisco Nexus 1010-X has the product ID (PID) N1K-C1010-X.

- You have upgraded the firmware using the Cisco Host Upgrade Utility (HUU). The HUU is a tool that upgrades the following components:
 - Cisco Integrated Management Controller (CIMC)
 - System BIOS
 - LAN on motherboard (LOM)
 - Cisco UCS P81E Virtual Interface Card (VIC)
 - Cisco UCS VIC 1225
 - Cisco UCS VIC 1225-T
 - Network adapters
 - LSI

Use the following Host Upgrade Utility version to upgrade the firmware before you upgrade the Cisco Nexus Virtual Services Appliance:

- For Cisco Nexus 1010 product family, see the [Cisco Host Upgrade Utility Release 1.4\(3\) Quick Start Guide](#).



Caution

It is a recommended Cisco best practice to upgrade the firmware using the **Cisco Host Upgrade Utility**. Failing to do so might result in network setup failure and/or system reboots. For information on the Cisco Host Upgrade Utility, see [Cisco Host Upgrade Utility Information, page 2-3](#).

- You are logged in to the CLI from the CIMC/Serial over LAN port on the rear of the Cisco Nexus Virtual Services Appliance.



Note

Do not log in using the management IP for this procedure. This procedure requires you to first upgrade and reload the standby Cisco Nexus Virtual Services Appliance after which the HA pair have incompatible software versions. By logging in using serial over LAN, you prevent the split brain that occurs in this configuration.

- You have already saved a backup copy of your running configuration on an external server.
- You have saved a copy of the new Cisco Nexus Virtual Services Appliance software file from the following Cisco.com software download site to an external server.
www.cisco.com/go/1010download
- You must have Cisco Integrated Management Controller (CIMC) Software Version 1.4(3s)4 or higher for Cisco Nexus 1010 product family installed. For more information, see the [Verifying the CIMC Software Version, page 2-4](#).

Send document comments to nexus1k-docfeedback@cisco.com.

Guidelines and Limitations

Follow these guidelines and limitations when upgrading the Cisco Nexus Virtual Services Appliance product family:

- This procedure upgrades both the active and standby Cisco Nexus Virtual Services Appliance.
- After reloading the new software version during an upgrade, you must save the new upgrade configuration persistently through reboots and restarts by copying it to the startup configuration. These procedures include a step for this.
- The only way to upgrade the software is by using the **install nexus1010** command
- Boot variables must be set by the system when you use the install command. Never attempt to set the boot variables manually.

Upgrading from Software Release 4.2(1)SP1(3) or Later

You can use this procedure for the following Cisco Nexus Virtual Services Appliance upgrade while retaining operational data and persistent information.

From software version	To software version
4.2(1)SP1(3)	4.2(1)SP1(5.1)
4.2(1)SP1(4)	



Note

Upgrade from 4.2(1)SP1(1) or 4.2(1)SP1(2) to 4.2(1)SP1(5.1) is not supported.



Note

For information about upgrading Cisco Nexus 1000V software on a VSB, see the *Cisco Nexus 1000V Software Installation and Upgrade Guide, Release 4.2(1)SV1(5.2)*.

DETAILED STEPS

- Step 1** From the Cisco Nexus Virtual Services Appliance serial over LAN connection, copy any unsaved configuration from the running configuration to startup so that it is preserved after the reload.

copy running-config startup-config

Example:

```
switch# copy running-config startup-config
[#####] 100%
switch#
```

- Step 2** Copy the new software image from the external server to the following directory.

bootflash: \repository

copy scp://user@path/filename bootflash:filename

Example:

```
switch# copy scp://user@linux-box.cisco.com/home/user/nexus-1010.4.2.1.SP1.5.1.iso
bootflash:repository
```

Send document comments to nexus1k-docfeedback@cisco.com.

```

Enter vrf (If no input, current vrf 'default' is considered):
user@linux-box.cisco.com's password:
nexus-1010.4.2.1.SP1.5.1.iso      100% 258234 10.3KB/s  00:15
switch#

```

Step 3 Install the new image.

install nexus1010 full_path_to_filename

Example:

```
switch# install nexus1010 bootflash:repository/nexus-1010.4.2.1.sp1.5.1.iso
```

The following things occur on the switch:

- The new software image is copied to bootflash and the standby Cisco Nexus Virtual Services Appliance is upgraded.
- Bootflash variables are updated with the names of the new system and kickstart images.
- The new image and bootflash variable information is saved in the startup configuration.
- The active reloads the standby with the new software version.
- The system waits for all VSBs to come up before the standby takes over and reloads the active with the new software version.

Step 4 From the CLI for each module, verify that both modules are in HA mode.

show system redundancy status

Example:

```

switch# show system redundancy status
Redundancy role
-----
      administrative:  primary
      operational:    primary
Redundancy mode
-----
      administrative:  HA
      operational:    None
This supervisor (sup-1)
-----
      Redundancy state: Active
      Supervisor state: Active
      Internal state:  Active with HA standby
Other supervisor (sup-2)
-----
      Redundancy state: standby
      Supervisor state: HA standby
      Internal state:  HA standby
switch#
-----

```

Step 5 Verify that the new software is loaded.

show module

```

switch# show module
Mod Ports  Module-Type                Model  Status
-----
 1     0      Cisco Virtual Services Appliance  VSA   active *
 2     0      Cisco Virtual Services Appliance  VSA   ha-standby

Mod Sw                Hw
-----
 1   4.2(1)SP1(5.1)     0.0
 2   4.2(1)SP1(5.1)     0.0

```

Send document comments to nexus1k-docfeedback@cisco.com.

```
Mod  MAC-Address(es)                               Serial-Num
---  -
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
2    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
```

```
Mod  Server-IP      Server-UUID  Server-Name
---  -
1    10.78.109.100   NA          NA
2    10.78.109.100   NA          NA
```

* this terminal session

Step 6 Save the new upgrade configuration persistently through reboots and restarts by copying it to the startup configuration.

copy running-config startup-config

Example:

```
switch# copy running-config startup-config
[#####] 100%
switch#
```

Upgrade Example

The following is an example of upgrade from software version 4.2(1)SP1(3) to 4.2(1)SP1(5.1).

```
login as: admin
Nexus 1010
Using keyboard-interactive authentication.
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

```
switch# show mod[15D[J
switch# show mod[Jule
```

```
Mod  Ports  Module-Type                               Model                               Status
---  -
1    0      Nexus 1010 (Virtual Services App)      Nexus1010                           active *
2    0      Nexus 1010 (Virtual Services App)      Nexus1010                           ha-standby
```

```
Mod  Sw                               Hw
---  -
1    4.2(1)SP1(3)                    0.0
2    4.2(1)SP1(3)                    0.0
```

```
Mod  MAC-Address(es)                               Serial-Num
---  -
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
2    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
```

Send document comments to nexus1k-docfeedback@cisco.com.

```

Mod  Server-IP      Server-UUID      Server-Name
---  -
1    10.78.109.59   NA               NA
2    10.78.109.59   NA               NA

* this terminal session
switch# show
switch# dir boot
switch# dir bootflash:r
switch# dir bootflash:r[Jepository

16384      Jun 11 02:49:38 2014  lost+found/
305928192  Jun 12 12:33:09 2014  nexus-1010.4.2.1.SP1.5.0.33.iso

Usage for bootflash://sup-local
308862976 bytes used
3682516992 bytes free
3991379968 bytes total

switch# inst
switch# inst nexu
switch# install nexu boot
switch# install nexus1010 boot[Jflash:[35D[J
switch# install nexus1010 bootflash:

bootflash:///                bootflash://sup-1/        bootflash://sup-local/

bootflash://module-1/       bootflash://sup-2/        bootflash://sup-remote/

bootflash://module-2/       bootflash://sup-active/   bootflash://sup-standby/
[J
switch# install nexus1010 bootflash://[J[Jr[36D[J
switch# install nexus1010 bootflash:r[Jepository/nexu[50D[J
switch# install nexus1010 bootflash:repository/nexu[Js-1010.4.2.1.SP1.5.0.33.iso

cpa_mgr debug: Using URI: bootflash:/repository/nexus-1010.4.2.1.SP1.5.0.33.iso
Installing bootflash:/repository/nexus-1010.4.2.1.SP1.5.0.33.iso
.....
Verifying image bootflash:/nexus-1010-kickstart-mz.4.2.1.SP1.5.1.bin for boot variable
"kickstart".
[#                ] 0%[#####] 100% -- SUCCESS

Verifying image bootflash:/nexus-1010-mz.4.2.1.SP1.5.1.bin for boot variable "system".
[#                ] 0%..[#####] 100% -- SUCCESS

Verifying image type.
[#                ] 0%[#####] 20%.[#####]
30%[#####] 40%[#####] 50%..[#####]
50%[#####] 50%.[#####] 90%[#####]
100%[#####] 100% -- SUCCESS

Extracting "system" version from image bootflash:/nexus-1010-mz.4.2.1.SP1.5.1.bin.
[#                ] 0%.[#####] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:/nexus-1010-kickstart-mz.4.2.1.SP1.5.1.bin.
[#                ] 0%[#####] 100% -- SUCCESS
.....
Notifying services about system upgrade.
.....[#####] 100% -- SUCCESS

Compatibility check is done:
Module bootable      Impact  Install-type  Reason
-----

```

Send document comments to nexus1k-docfeedback@cisco.com.

```

1      yes non-disruptive      reset
2      yes non-disruptive      reset

```

Images will be upgraded according to following table:

Module	Image	Running-Version	New-Version	Upg-Required
1	system	4.2(1)SP1(3)	4.2(1)SP1(5.1)	yes
1	kickstart	4.2(1)SP1(3)	4.2(1)SP1(5.1)	yes
2	system	4.2(1)SP1(3)	4.2(1)SP1(5.1)	yes
2	kickstart	4.2(1)SP1(3)	4.2(1)SP1(5.1)	yes

Module	Running-Version	ESX Version
VSM Compatibility	ESX Compatibility	

Install is in progress, please wait.

```

Syncing image bootflash:/nexus-1010-kickstart-mz.4.2.1.SP1.5.1.bin to standby.
[#          ] 0%.[#####] 100% -- SUCCESS

```

```

Syncing image bootflash:/nexus-1010-mz.4.2.1.SP1.5.1.bin to standby.
[#          ] 0%..[#####] 100% -- SUCCESS

```

```

Setting boot variables.
[#          ] 0%...[#####] 100% -- SUCCESS

```

```

Performing configuration copy.
[#          ] 0%[##          ] 5%[###          ] 10%[####          ]
] 15%[#####          ] 35%[#####          ] 40%[#####          ]
45%[#####          ] 50%[#####          ] 70%[#####          ]
75%[#####          ] 80%[#####          ] 85%[#####          ]
100%.[#####] 100% -- SUCCESS
.....2014 Jun 12 12:37:03 n1010 %PLATFORM-2-MOD_REMOVE: Module 2 removed
(Serial number T023D7FFD81)

```

```

.....
.....2014 Jun 12 12:40:41 n1010 %PLATFORM-2-MOD_DETECT: Module 2 detected
(Serial number :unavailable) Module-Type Virtual Supervisor Module Model :unavailable

```

```

.....
Module 2: Waiting for module online.
-- SUCCESS

```

```

.....
Notifying services about the switchover.
.[#####] 100% -- SUCCESS

```

```

"Switching over onto standby".
login as: admin
Nexus 1010
Using keyboard-interactive authentication.
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2012, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and

```

Send document comments to nexus1k-docfeedback@cisco.com.

<http://www.opensource.org/licenses/lgpl-2.1.php>

```
switch# show mod[15D[J
switch# show mod[Jule
```

Mod	Ports	Module-Type	Model	Status
1	0	Cisco Virtual Services Appliance	VSA	ha-standby
2	0	Cisco Virtual Services Appliance	VSA	active *

Mod	Sw	Hw
1	4.2(1)SP1(5.1)	0.0
2	4.2(1)SP1(5.1)	0.0

Mod	MAC-Address(es)	Serial-Num
1	00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8	NA
2	00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8	NA

Mod	Server-IP	Server-UUID	Server-Name
1	10.78.109.59	NA	NA
2	10.78.109.59	NA	NA

* this terminal session

The following is an example of upgrade from software version 4.2(1)SP1(3) to 4.2(1)SP1(4).

```
cppa_mgr# install nexus1010 bootflash:repository/nexus-1010.4.2.1.SP1.4.iso
cppa_mgr debug: Using URI: bootflash:/repository/nexus-1010.4.2.1.SP1.4.iso
Installing bootflash:/repository/nexus-1010.4.2.1.SP1.4.iso
.....
Verifying image bootflash:/nexus-1010-kickstart-mz.4.2.1.SP1.4.bin for boot variable
"kickstart".
[[#####] 100% -- SUCCESS

Verifying image bootflash:/nexus-1010-mz.4.2.1.SP1.4.bin for boot variable "system".
[[#####] 100% -- SUCCESS

Verifying image type.
[[[[#####] 100% -- SUCCESS

Extracting "system" version from image bootflash:/nexus-1010-mz.4.2.1.SP1.4.bin.
[[#####] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:/nexus-1010-kickstart-mz.4.2.1.SP1.4.bin.
[[#####] 100% -- SUCCESS
.....
Notifying services about system upgrade.                                [#####]
100% -- SUCCESS
.
Compatibility check is done:
Module bootable          Impact  Install-type  Reason
-----
      1      yes  non-disruptive      reset
      2      yes  non-disruptive      reset

Images will be upgraded according to following table:
Module      Image      Running-Version      New-Version  Upg-Required
-----
```


Send document comments to nexus1k-docfeedback@cisco.com.

Module	Running-Version	ESX Version	VSM Compatibility	ESX Compatibility
1	system	4.2(1)SP1(3)	4.2(1)SP1(4)	yes
1	kickstart	4.2(1)SP1(3)	4.2(1)SP1(4)	yes
2	system	4.2(1)SP1(3)	4.2(1)SP1(4)	yes
2	kickstart	4.2(1)SP1(3)	4.2(1)SP1(4)	yes

Install is in progress, please wait.

Syncing image bootflash:/nexus-1010-kickstart-mz.4.2.1.SP1.4.bin to standby.
[#####] 100% -- SUCCESS

Syncing image bootflash:/nexus-1010-mz.4.2.1.SP1.4.bin to standby.
[#####] 100% -- SUCCESS

Setting boot variables.
[# [#####] 100% -- SUCCESS

Performing configuration copy.
[[#####] 100% -- SUCCESS
.....2011 Jul 25 20:12:16 cppa-mgr %PLATFORM-2-MOD_REMOVE: Module 2 removed (Serial number T023D750981)
.....2011 Jul 25 20:14:54 cppa-mgr %PLATFORM-2-MOD_DETECT: Module 2 detected (Serial number :unavailable)
Module-Type Virtual Supervisor Module Model :unavailable
.....
Module 2: Waiting for module online.
-- SUCCESS

Notifying services about the switchover.
[#####] 100% -- SUCCESS

"Switching over onto standby".

Broadcast message from root (console) (Mon Jul 25 20:20:41 2011):

The system is going down for reboot NOW!
INIT: Switching to runlevel: 6
INIT: Sending processes the TERM signal
Jul 25 20:20:41 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "sksd" (PID 2487) is forced exit.
Jul 25 20:20:41 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "Security Daemon" (PID 2499) is forced exit.
Jul 25 20:20:41 %TTYD-2-TTYD_ERROR TTYD Error ttyd bad select
Jul 25 20:20:41 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "stp" (PID 2765) is forced exit.
Jul 25 20:20:41 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "fs-daemon"(PID2455)is forced exit.
Jul 25 20:20:41 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "Cert_enroll Daemon"(PID 2500)is forced exit.
Jul 25 20:20:41 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "netstack"(PID2557)is forced exit.
Jul 25 20:20:41 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "vdc_mgr"(PID 2484)is forced exit.
Jul 25 20:20:41 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "u6rib" (PID 2507) is forced exit.
Jul 25 20:20:41 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "res_mgr"(PID 2489)is forced exit.
Jul 25 20:20:41 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "licmgr" (PID 2454)is forced exit.
Jul 25 20:20:41 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "igmp" (PID 2771) is forced exit.
Jul 25 20:20:41 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "adjmgr" (PID 2537)is forced exit.
Jul 25 20:20:41 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "Radius Daemon"(PID 2634)is forced exit.
Jul 25 20:20:41 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "AAA Daemon"(PID 2501)is forced exit.
Jul 25 20:20:41 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "urib" (PID 2508) is forced exit.
Auto booting bootflash:/nexus-1010-kickstart-mz.4.2.1.SP1.4.bin bootflash:/nexus-1010-mz.4.2.1.SP1.3.bin...
Booting kickstart image: bootflash:/nexus-1010-kickstart-mz.4.2.1.SP1.4.bin.

Send document comments to nexus1k-docfeedback@cisco.com.

```

.....Image verification
OK

Starting kernel...
PCI: PIIX3: Enabling Passiv%H+Y4%
                                001-Usage: init 0123456SsQqAaBbCcUu
mkdir: cannot create directory `/new-root/old-root': File exists
INIT: version 2.85 booting
Bootflash device is /dev/hda
Checking all filesystems..... done.
Setting kernel variables: sysctlnet.ipv4.ip_forward = 0
net.ipv4.ip_default_ttl = 64
net.ipv4.ip_no_pmtu_disc = 1
.
/etc/rc.d/rcS.d/S35iptables: line 41: //iptables: No such file or directory
/etc/rc.d/rcS.d/S35iptables: line 44: //ip6tables: No such file or directory
Loading system software
Uncompressing system image: bootflash:/nexus-1010-mz.4.2.1.SP1.4.bin

Load plugins that defined in image conf: /isan/plugin_img/img.conf
load_plugin: failed read swid map from "/mnt/pss/plugin_swid_map" with rc 0xffffffff.
Plugin will be assigned new ID
Loading plugin 0: core_plugin...
load_plugin: Can't get exclude list from /isan/plugin/0/boot/etc/plugin_exclude.conf (rc
0x40ea0017)
plugin_link_to_exec_path: plugin_path = /isan/plugin/0, tar_log =
/isan/plugin_extract_log/0
num srgs 1
0: swid-core-suplsfp, swid-core-suplsfp
num srgs 1
0: swid-suplsfp-ks, swid-suplsfp-ks
INIT: Entering runlevel: 3
Starting dhcpd daemon: dhcpdInternet Systems Consortium DHCP Server V3.0.1rc14
Copyright 2004 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/
Wrote 0 deleted host decls to leases file.
Wrote 0 new dynamic host decls to leases file.
Wrote 0 leases to leases file.

Not configured to listen on any interfaces!
.
Exporting directories for NFS kernel daemon...done.
Starting NFS kernel daemon:rpc.nfsd.
rpc.mountddone.

/bin/mkdir: cannot create directory `/bootflash/repository': File exists
/isan/bin/mount_cpparepository exist

Nexus 1010
cppa-mgr(standby) login: 2011 Jul 26 04:24:22 cppa-mgr %USER-2-SYSTEM_MSG: CLIS: loading
cmd files begin - clis
2011 Jul 26 04:24:29 cppa-mgr %USER-2-SYSTEM_MSG: CLIS: loading cmd files end - clis
2011 Jul 26 04:24:29 cppa-mgr %USER-2-SYSTEM_MSG: CLIS: init begin - clis
2011 Jul 26 04:24:38 cppa-mgr %USER-2-SYSTEM_MSG: Invalid feature name eth-port-sec - clis
Nexus 1010
cppa-mgr(standby) login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2012, Cisco Systems, Inc. All rights reserved.

```

Send document comments to nexus1k-docfeedback@cisco.com.

```
The copyrights to certain works contained in this software are owned by other third
parties and used and distributed under license. Certain components of this software are
licensed under the GNU General Public License (GPL) version 2.0 or the GNU Lesser General
Public License (LGPL) Version 2.1. A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
coppa-mgr(standby)#
```

```
Inactive timeout reached, logging out.
```

```
Nexus 1010
coppa-mgr(standby) login:
(The upgrade of the standby Cisco Nexus 1010 begins here.)
```

```
Auto booting bootflash:/nexus-1010-kickstart-mz.4.2.1.SP1.4.bin
bootflash:/nexus-1010-mz.4.2.1.SP1.4.bin...
Booting kickstart image: bootflash:/nexus-1010-kickstart-mz.4.2.1.SP1.4.bin.
.....Image verification
OK
```

```
Starting kernel...
PCI: PIIX3: Enabling Passive Veh+001-?Usage: init 0123456SsQqAaBbCcUu
mkdir: cannot create directory `/new-root/old-root': File exists
INIT: version 2.85 booting
Bootflash device is /dev/hda
Checking all filesystems...r.r.r done.
```

```
Setting kernel variables: sysctlnet.ipv4.ip_forward = 0
net.ipv4.ip_default_ttl = 64
net.ipv4.ip_no_pmtu_disc = 1
.
/etc/rc.d/rcS.d/S35iptables: line 41: //iptables: No such file or directory
/etc/rc.d/rcS.d/S35iptables: line 44: //ip6tables: No such file or directory
Loading system software
Uncompressing system image: bootflash:/nexus-1010-mz.4.2.1.SP1.4.bin
```

```
Load plugins that defined in image conf: /isan/plugin_img/img.conf
load_plugin: failed read swid map from "/mnt/pss/plugin_swid_map" with rc 0xffffffff.
Plugin will be assigned new ID
Loading plugin 0: core_plugin...
load_plugin: Can't get exclude list from /isan/plugin/0/boot/etc/plugin_exclude.conf (rc
0x40ea0017)
plugin_link_to_exec_path: plugin_path = /isan/plugin/0, tar_log =
/isan/plugin_extract_log/0
num srgs 1
0: swid-core-suplsfp, swid-core-suplsfp
num srgs 1
0: swid-suplsfp-ks, swid-suplsfp-ks
INIT: Entering runlevel: 3
Starting dhcpd daemon: dhcpdInternet Systems Consortium DHCP Server V3.0.1rc14
Copyright 2004 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/
Wrote 0 deleted host decls to leases file.
Wrote 0 new dynamic host decls to leases file.
Wrote 0 leases to leases file.
```

```
Not configured to listen on any interfaces!
```

```
.
Exporting directories for NFS kernel daemon...done.
Starting NFS kernel daemon:rpc.nfsd.
rpc.mountddone.
```

```
/bin/mkdir: cannot create directory `/bootflash/repository': File exists
```

Send document comments to nexus1k-docfeedback@cisco.com.

```

/isan/bin/mount_cpp_a_repository exist

Continuing with installation, please wait
Trying to start the installer...
Trying to start the installer...
2012 May 26 09:30:15 cppa-mgr %USER-2-SYSTEM_MSG: CLIS: loading cmd files end - clis
2012 May 26 09:30:15 cppa-mgr %USER-2-SYSTEM_MSG: CLIS: init begin - clis
2012 May 26 09:30:32 cppa-mgr %USER-2-SYSTEM_MSG: Invalid feature name eth-port-sec - clis

Module 2: Waiting for module online.
-- SUCCESS
2011 Jul 25 20:20:41 cppa-mgr %SYSMGR-2-HASWITCHOVER_PRE_START: This supervisor is
becoming active (pre-start phase).
2011 Jul 25 20:20:41 cppa-mgr %SYSMGR-2-HASWITCHOVER_START: This supervisor is becoming
active.
2011 Jul 25 20:20:41 cppa-mgr %SYSMGR-2-SWITCHOVER_OVER: Switchover completed.
2011 Jul 25 20:20:58 cppa-mgr %PLATFORM-2-MOD_REMOVE: Module 1 removed (Serial number )

2011 Jul 25 20:24:21 cppa-mgr %PLATFORM-2-MOD_DETECT: Module 1 detected (Serial number
:unavailable) Module-Type Virtual Supervisor Module Model :unavailable
Install has been successful.

Nexus 1010
cppa-mgr login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2012, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are owned by other third
parties and used and distributed under license. Certain components of this software are
licensed under the GNU General Public License (GPL) version 2.0 or the GNU Lesser General
Public License (LGPL) Version 2.1. A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
cppa-mgr# copy running-config startup-config
[#####] 100%
cppa-mgr#

```

Feature History for Software Upgrade

This section provides the software installation and upgrade release history.

Feature Name	Releases	Feature Information
Software upgrade	4.2(1)SP1(2)	This feature was introduced.



CHAPTER 4

Cisco Nexus Virtual Services Appliance Software Reinstallation

This chapter describes how to reinstall the Cisco Nexus Virtual Services Appliance software, and includes the following sections:

- [Reinstalling Cisco Nexus Virtual Services Appliance](#)
- [Replacing a Cisco Nexus Virtual Services Appliance](#)
- [Feature History for Software Reinstallation](#)

Reinstalling Cisco Nexus Virtual Services Appliance

This section contains the following topics:

- [Information About Reinstalling the Software](#)
- [Guidelines and Limitations](#)
- [Reinstalling the Software](#)

Information About Reinstalling the Software

You can reinstall a different version of the software on Cisco Nexus Virtual Services Appliance product family in any one of the following cases:

- The Cisco Nexus Virtual Services Appliance disk gets corrupted.
- The latest version of Cisco Nexus Virtual Services Appliance has been shipped to you, but you want to install the previous version of the software.

In the event of disk corruption on the Cisco Nexus Virtual Services Appliance, the system can be brought up by copying the image from a CD.

Guidelines and Limitations

Use the following guidelines and limitations when reinstalling the software:



Caution

When you reinstall the software, all previous configuration is overwritten and lost.

[Send document comments to nexus1k-docfeedback@cisco.com.](mailto:nexus1k-docfeedback@cisco.com)

Reinstalling the Software

You can use this procedure to reinstall the software from your software CD in the event that the system disk becomes corrupted.

BEFORE YOU BEGIN

Before beginning this procedure you must know or do the following:

- You have verified that you have the following product ID (PID), using the [“Verifying the CIMC Software Version” procedure on page 2-4.](#)
 - N1K-C1010 on Cisco Nexus 1010
 - N1K-C1010-X on Cisco Nexus 1010-X



Caution

You cannot install or upgrade to Release 4.2(1)SP1(5.1) unless your Cisco Nexus 1010 has the product ID (PID) N1K-C1010 or your Cisco Nexus 1010-X has the product ID (PID) N1K-C1010-X.



Caution

Potential Loss of Data

When you reinstall the software, all previous configuration is overwritten and lost.

DETAILED STEPS

-
- Step 1** From a terminal server, connect to the serial port of the Cisco Nexus Virtual Services Appliance.
- Step 2** Insert the installation CD in the DVD-RW drive.
- Step 3** On the Cisco Nexus Virtual Services Appliance, press the Power button.
- The Cisco Nexus Virtual Services Appliance reboots and the management software setup process begins. To configure the software, see the *Cisco Nexus Virtual Services Appliance Software Configuration Guide, Release 4.2(1)SP1(5.1)*.
-

Replacing a Cisco Nexus Virtual Services Appliance

You can replace one Cisco Nexus Virtual Services Appliance in a redundant pair using the process shown in the flowchart in [Figure 4-1 on page 4-5.](#)



Note

For information about powering down, disconnecting, repacking, and shipping the Cisco Nexus Virtual Services Appliance, refer to the *Cisco Nexus Virtual Services Appliance Hardware Installation Guide*.

Send document comments to nexus1k-docfeedback@cisco.com.

BEFORE YOU BEGIN

Before setting up the software for a replacement Cisco Nexus Virtual Services Appliance, you must know or do the following:

Step 1 Collect the following information from the functioning Cisco Nexus Virtual Services Appliance.

- Software version
- HA role

The HA role of the functioning Cisco Nexus Virtual Services Appliance determines the role assigned to the replacement Cisco Nexus Virtual Services Appliance.

- If the functioning Cisco Nexus Virtual Services Appliance is in the primary HA role, the software for the replacement Cisco Nexus Virtual Services Appliance must be set up in the secondary HA role.
- If the functioning Cisco Nexus Virtual Services Appliance is in the secondary HA role, the software for the replacement Cisco Nexus Virtual Services Appliance must be set up in the primary HA role.

- Control VLAN
- Management VLAN
- Domain ID
- Network uplink type

When setting up the software for the replacement Cisco Nexus Virtual Services Appliance, you must use the same IDs used on the functioning Cisco Nexus Virtual Services Appliance.

Step 2 Prepare the replacement Cisco Nexus Virtual Services Appliance by doing the following:

- a. Perform a total firmware update. See [Prerequisites, page 2-2](#).
 - Verify the firmware ISO image.
- b. Install the same software version on the replacement Cisco Nexus Virtual Services Appliance as that on the existing Cisco Nexus Virtual Services Appliance.
 - The software versions running on the functioning Cisco Nexus Virtual Services Appliance and the replacement Cisco Nexus Virtual Services Appliance must match. The replacement Cisco Nexus Virtual Services Appliance has the latest software version installed on it when it is shipped.
 - If you need to downgrade the software version on the replacement Cisco Nexus Virtual Services Appliance, use the procedure in the [Information About Reinstalling the Software, page 4-1](#).
 - If you need to upgrade the software on one of the Cisco Nexus Virtual Services Appliances, use the procedure in the [Upgrading from Software Release 4.2\(1\)SP1\(3\) or Later, page 3-3](#).

Step 3 Connect the replacement Cisco Nexus Virtual Services Appliance to the upstream switch. See the *Cisco Nexus Virtual Services Appliance Hardware Installation Guide* for information about connecting to upstream switches.

Step 4 On the existing Virtual Supervisor Module (VSM), do the following:

- Get the following information:
 - VSM version
 - Domain ID
 - Management IP address

Send document comments to nexus1k-docfeedback@cisco.com.

- IP subnet mask
- Gateway IP address
- Check that the corresponding ISO image is present. If it is not present, bring it in.

show bootflash:repository

```
switch# dir bootflash:repository
283129856    Apr 25 15:39:15 2012 nexus-1000v.4.2.1.SV1.5.1.iso
```

Step 5 After you set up the software for the replacement Cisco Nexus Virtual Services Appliance, you must manually enable the HA peer for each redundant virtual service blade (VSB). Refer to the *Cisco Nexus Virtual Services Appliance Software Configuration Guide, Release 4.2(1)SP1(5.1)*.

- If the functioning Cisco Nexus Virtual Services Appliance is in the primary HA role, enable the secondary HA peer for each redundant VSB.

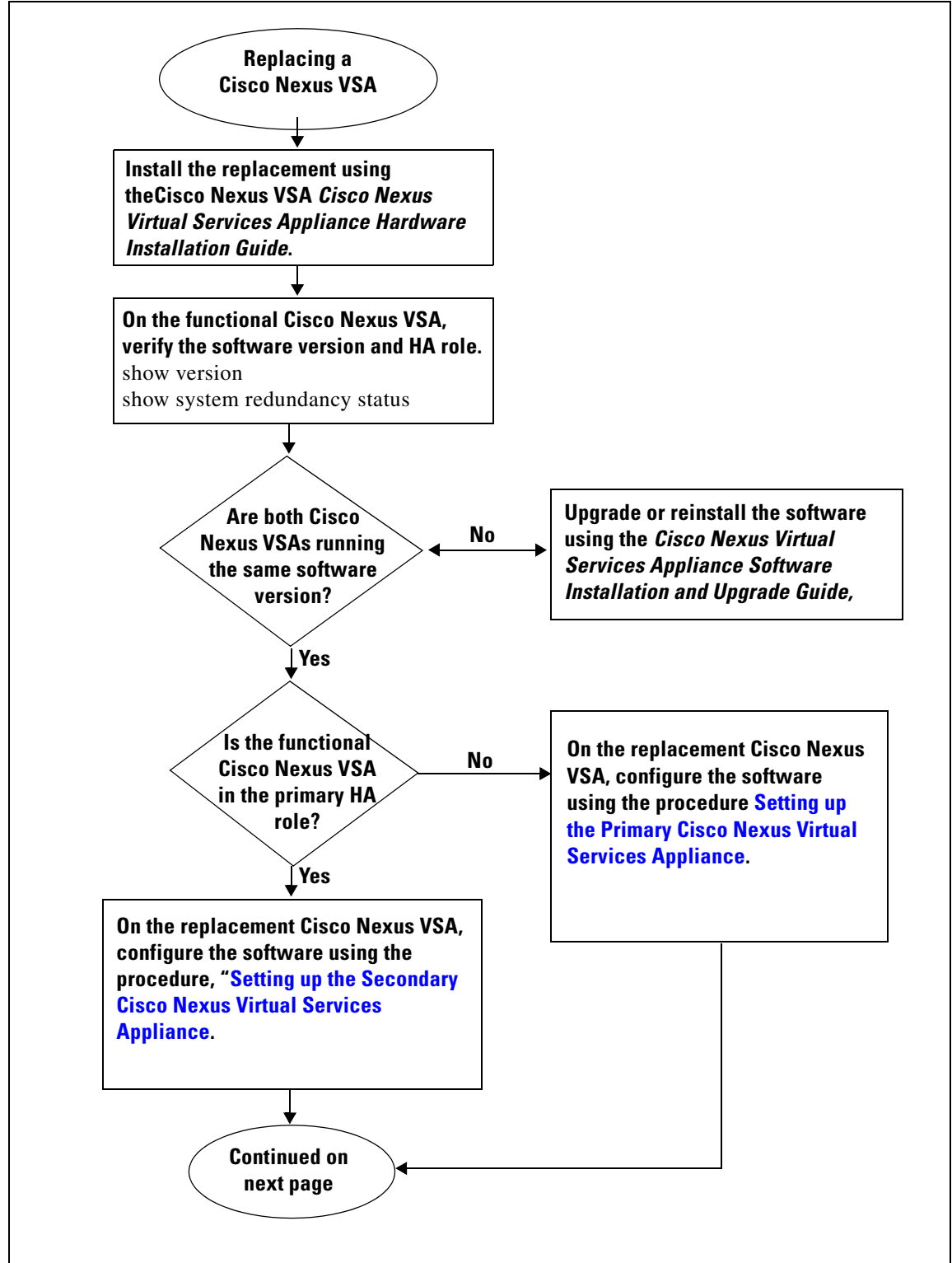
```
configure terminal
virtual-service-blade name
enable secondary
```

- If the functioning Cisco Nexus Virtual Services Appliance is in the secondary HA role, enable the primary HA peer for each redundant VSB.

```
configure terminal
virtual-service-blade name
enable primary
```

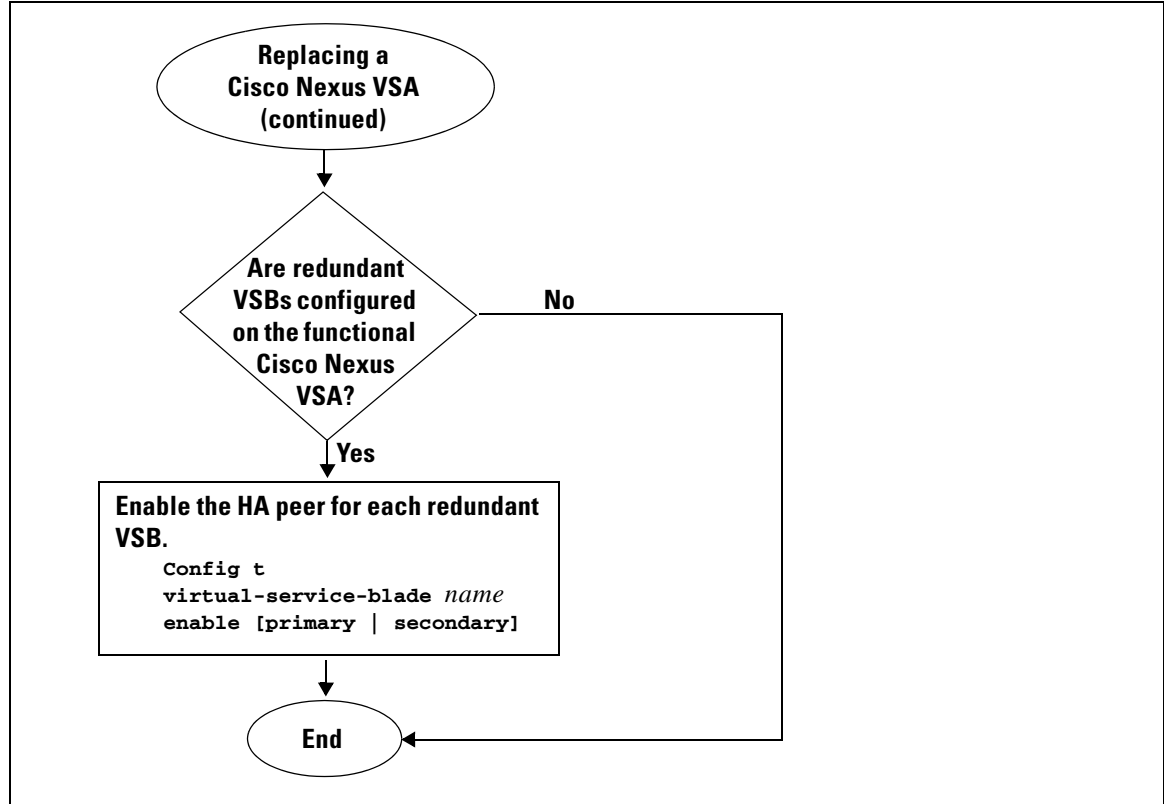

Send document comments to nexus1k-docfeedback@cisco.com.

Figure 4-1 Flow Chart: Replacing a Cisco Nexus Virtual Services Appliance



Send document comments to nexus1k-docfeedback@cisco.com.

Figure 4-2 Flow Chart: Replacing a Cisco Nexus Virtual Services Appliance (continued)



Feature History for Software Reinstallation

This section provides the software reinstallation release history.

Feature Name	Releases	Feature Information
Software reinstall or upgrade	4.2(1)SP1(2)	This feature was introduced.



INDEX

A

appliance name
 CLI setup [2-13](#)
audience [iii-v](#)

C

CIMC
 information about [1-1](#)
CLI prompt, appliance [2-13](#)
control and packet VLAN
 about [2-8](#)
 CLI setup [2-10, 2-16](#)
conventions [iii-vi](#)

D

default gateway
 CLI setup [2-13](#)
documentation
 additional publications [iii-vii](#)
 related documents [iii-vi](#)

F

Flow Chart
 Replacing a Cisco Nexus 1010 [2-24](#)

H

HA
 redundancy role [2-6](#)

redundancy state [2-7](#)

M

management software
 verify setup [2-18](#)
management VLAN
 about [2-8](#)
 CLI setup [2-11, 2-16](#)
mgmt0
 CLI setup [2-13](#)

N

name, appliance [2-13](#)
NTP
 CLI setup [2-13](#)

P

password strength [2-6](#)
ports, uplinks [2-8](#)
prompt, CLI [2-13](#)

R

redundancy
 role [2-6](#)
 state [2-7](#)
related documents [iii-vii, iii-viii](#)
replacing a Cisco Nexus 1010 [2-21](#)

Send document comments to nexus1k-docfeedback@cisco.com.

S

SSH

CLI setup [2-13](#)

strong password [2-6](#)

T

Telnet

CLI setup [2-13](#)

U

uplinks

CLI setup [2-16](#)

port and VLAN assignments [2-8](#)

V

verify

management software setup [2-18](#)

VLAN

about [2-8](#)

uplink port assignments [2-8](#)