Netcrypt Bulk Encryptor Software

Installation Instructions

Please Read

Important

Please read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgements

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 proprty of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

Copyright

Contents

About This Guide

Introduction

This document provides procedures for installing software on a Netcrypt™ Bulk Encryptor in non-Overlay and Overlay™ environments. This document also contains instructions for restoring the previous software version in the unlikely event that the upgrade is not successful.

Important: Use this document in conjunction with the release notes for the software version that you are installing. The release notes provide information about the software such as new features, compatibility with system releases, and the installation media and tools.

Scope

This document provides instructions for installing software on a Netcrypt. It does not provide instructions for installing Netcrypt hardware in your headend.

Audience

This document is written for installers, operators and technicians, and field service engineers.

Document Version

This is the third release of this guide.

This guide was revised to include information on downloading software from Cisco.com.

1

Preparing to Upgrade the Software

Introduction

Before installing the software, there are several tasks that you must complete to ensure a successful installation. This chapter provides instructions on how to complete those tasks.

In This Chapter

Upgrade Process Overview

This section provides an overview of upgrade tasks. It also provides information that is critical to a successful upgrade, such as how the upgrade impacts subscribers and ways to minimize its impact on subscribers. Read this section before attempting to upgrade the software.

Before You Begin

Before you upgrade the software, be sure that your system meets the criteria specified in the Netcrypt Bulk Encryptor software release notes.

Time to Complete

When upgrading Netcrypt Bulk Encryptors with new software, consider the following tasks and the amount of time required for each:

- Completing pre-upgrade tasks takes from 30 to 45 minutes.
- Downloading software from Cisco.com takes from 10 to 15 minutes. The speed of the connection and the size of the files will determine the actual download time.
- Downloading new software to a Netcrypt Bulk Encryptor takes approximately 5 to 10 minutes for each device.
- For Netcrypt Bulk Encryptors that encrypt broadcast sessions, the DNCS will restart the sessions after the Netcrypt Bulk Encryptors load new software.
- For Netcrypt Bulk Encryptors that encrypt VOD sessions, only those sessions determined to be active will be restarted. Since subscribers may tune away when the Netcrypt Bulk Encryptor reboots, the total number of recovered sessions may not match the original number of sessions on the Netcrypt Bulk Encryptors.

Note: It is not necessary to rebuild non-VOD sessions on the Netcrypt Bulk Encryptors that you upgrade. The non-VOD sessions are rebuilt automatically after the new software is downloaded to the Netcrypt Bulk Encryptor.

Subscriber Impact

When Netcrypt Bulk Encryptors are reset (rebooted) during the upgrade, the services they carry are temporarily interrupted. DHCTs will show a frozen picture or black screen until the upgrade is complete and the DNCS has restored all active sessions on the Netcrypt Bulk Encryptor.

Impact of TVs with QAM Tuners

When upgrading Netcrypt Bulk Encryptors to new releases of software, you must reset the Netcrypt Bulk Encryptors in order for the devices to download the new software from the DNCS. When the software download is complete, the DNCS then recreates any broadcast sessions that were sent to the Netcrypt Bulk Encryptors for encryption.

An increasing number of TVs are being manufactured and sold with QAM tuners that can access services that are not properly encrypted. Therefore, as a part of the upgrade process, we encourage you to verify that the DNCS re-establishes encryption for all secure services on the modulators that receive sessions from upgraded Netcrypt Bulk Encryptors. This extra step ensures that no modulator that may be carrying content inappropriate for children can be viewed inadvertently when using a TV that is equipped with a QAM tuner. For additional information, refer to the following procedures:

- ***Verifying the Functionality of Modulators That Carry Netcrypt-Encrypted Broadcast Sessions*** (on page 18)
- ***Verifying the Functionality of Modulators that Carry Netcrypt-Encrypted xOD or VOD Sessions*** (on page 19)

Process Overview

This section provides an overview of the software upgrade process.

Important: You should only upgrade to new releases of software if your network is running in a healthy state (for example, a system can boot and stage set-tops). If your network is not in a healthy state, you should not upgrade to the new release of software unless the new release contains a remedy to your system issue.

CAUTION:

If you are upgrading more than one Netcrypt Bulk Encryptor, download the new software to one group of devices (for example, all of the devices in a single rack or hub) and verify the functionality before attempting to download the software to another group of devices. Verifying the functionality of one group of devices at a time enables you to better isolate any failures that may occur and enables you to minimize service interruptions.

Pre-Upgrade Tasks

Important: Performing the pre-upgrade tasks will not impact system performance.

1. Verify that the install tool (install_pkg) exists on the DNCS.

   Note: For procedures on how to check for the install_pkg tool, see ***Verify the Install Package Exists on the DNCS*** (on page 23).
2. Determine the configuration (config) files currently in use on your system.
3. Verify the software version associated with the configuration files.

4 Make a backup copy of the *current* Netcrypt Bulk Encryptor configuration file.

5 If you are upgrading more than one Netcrypt Bulk Encryptor, establish an upgrading order.

6 Install the software onto the DNCS.

Upgrade Tasks

Important: Performing the upgrade tasks will result in a temporary loss of service as Netcrypt Bulk Encryptors are reset.

1 Download the new software to the Netcrypt Bulk Encryptors.

2 If the Netcrypt Bulk Encryptors you are upgrading currently carry broadcast sessions, determine the sessions that are running on those Netcrypt Bulk Encryptors you plan to upgrade. This will allow you to verify that these sessions are rebuilt after the new software is downloaded.

3 Verify that the upgraded Netcrypt Bulk Encryptor is functioning properly.

Important: Read and follow the appropriate directions contained in ***Impact of TVs with QAM Tuners*** (on page 3).

4 After the upgrade is complete, generate a Doctor Report using the **–av** option to verify system stability and functionality.

5 Perform system validation tests for your system release version.

Verify the Current Software Version on the DNCS

Introduction

Before attempting to upgrade the software, verify the number of configuration files in use and what software version is associated with each configuration file.

On occasion, for testing purposes, the configuration file for a test device or a set of test devices is changed to a non-standard value (for example nc111.config instead of nc.config). If your site has been involved in this type of testing (and you are now ready to use the released code again), you should update the configuration file setting for your test units to reflect the default values.

Note: The default configuration file varies according to the installation environment:

- In a non-Overlay environment, the default configuration file is **/tftpboot/nc.config**.
- In an Overlay environment, the default configuration is **/tftpboot/nobe.config**.

Failure to correct a unit from using a unique configuration will result in the unit remaining in the uniquely-specified configuration. Specifically, it will not load the new code and it will continue to load the code specified in the unique configuration file.

In extremely rare cases, the configuration file may have been specified in or may need to be specified in the /etc/bootptab file. In the event that a headend device fails to load the code you intended it to receive, you should check to see if a unique file was specified either through the DNCS GUI or in the /etc/bootptab file before contacting Cisco Services for assistance.

Checking for Multiple Config Files

Important: When using the DBAccess utility, take care to enter the commands as shown in the following procedure. Failure to enter the commands as shown may cause operational errors.

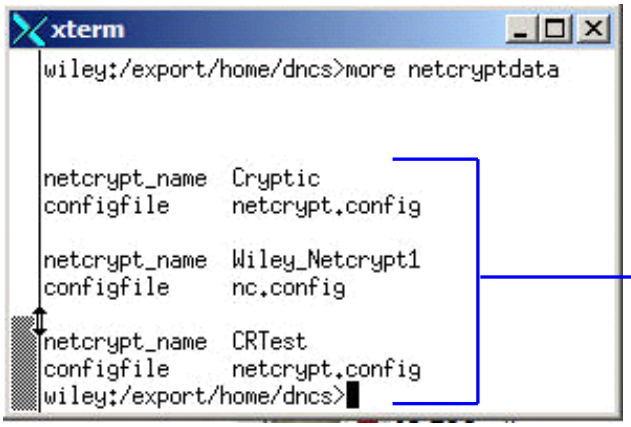
1. From the DNCS Administrative Console, click **Utilities** and click **xterm**. The xterm window opens.
2. Type **dbaccess dncsdb <<%** and press **Enter**.
3. Type **output to netcryptdata select netcrypt_name, configfile from netcrypt;** and press **Enter**.
4. Type % and press **Enter**. A result, similar to the following output, appears.

```
Database selected.

5 row(s) unloaded.

Database closed.
```

5 Type **more netcryptdata** and press **Enter**. A result, similar to the following output, appears.



6 Did more than one config file appear?

- If **yes**, keep the xterm window open and go to step 7.
- If **no**, go to *Checking the Software Version Associated with the config File* (on page 7).

7 Do you need to continue to run different versions of Netcrypt software on some Netcrypt Bulk Encryptors in your network?

- If **yes**, refer to *Load Multiple Versions of Netcrypt Code* (on page 25).
- If **no**, go to step 8.

8 Update the Netcrypt Bulk Encryptors to use the same config file by performing the following steps:

a From the DNCS Administrative Console, click **Network Element Provisioning** (If this tab is not present, click the **Element Provisioning** tab.) Then click **Netcrypt**. The Netcrypt List window opens.

b Select the Netcrypt Bulk Encryptor to upgrade and click **Edit**. The Update Netcrypt window opens.

c In the Netcrypt Provisioning area, modify the **Configuration File** field as needed.

- For a non-Overlay environment, enter **nc.config**.
- For an Overlay environment, enter **nobe.config**.

d Click **Save** to save this change. The system saves your changes and closes the Update Netcrypt window. The Netcrypt List window is now visible.

9 Go to *Checking the Software Version Associated with the config File* (on page 7).

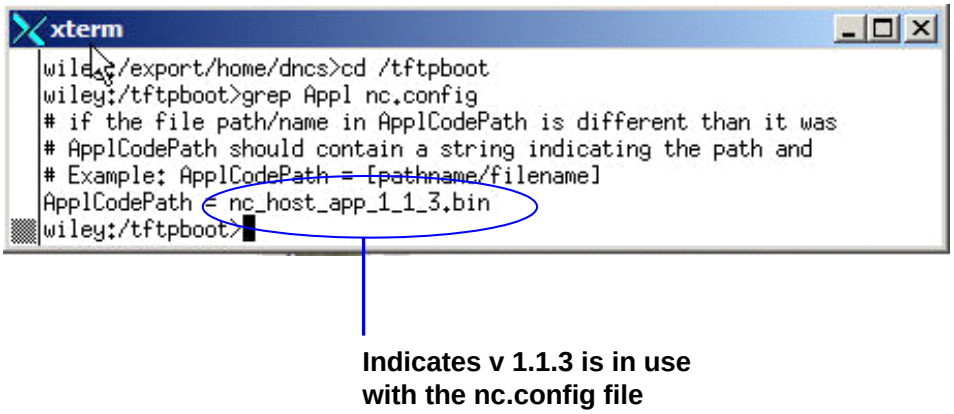
Checking the Software Version Associated with the config File

1 From the xterm window, type **cd /tftpboot** and press **Enter**. The tftpboot directory becomes the working directory.

2 For each unique config file identified in ***Checking for Multiple config Files*** (on page 5), type **grep Appl <config file name>** and press **Enter**.

Example: grep Appl nc.config

Result: A result, similar to the following output, appears.



Indicates v 1.1.3 is in use with the nc.config file

3 Is the proper version of software installed?

- If **yes**, type **exit** and press **Enter**.
- If **no**, go to ***Back Up the Current Netcrypt Configuration File*** (on page 8).

Back Up the Current Netcrypt Configuration File

Introduction

Before installing the new Netcrypt software, make a backup file of the config file currently installed on the DNCS by completing the following steps.

CAUTION:

Do not install new software until you have created a backup of the configuration file currently installed on your system. Having a backup file will enable you to restore the previous version of Netcrypt software in the unlikely event of a failure.

Restore the previous version of software to your system only when recommended by Cisco Services.

Backing Up the Current Netcrypt or NOBE Configuration File

1. Complete the following steps to log on to the xterm window as **root** user.
   a. Type **su -** and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
2. Type **cd /tftpboot** and press **Enter** to access the tftpboot directory.
3. Type **pwd** and press **Enter**. The /tftpboot directory name appears and indicates that you are in the correct directory.
4. Type the command suited for your environment:
   - For installations in a non-Overlay environment, type **cp –p nc.config nc.config<_software version number>** to copy the current configuration file to a backup file, and then press **Enter**.

     Example: Type **cp –p nc.config nc.config_1_1_3** and press **Enter.**
   - For installations in an Overlay environment, type **cp -p nobe.config nobe.config<_software version number>** to copy the current configuration file to a backup file, and then press **Enter**.

     Example: Type **cp -p nobe.config nobe.config_1_1_3** and press **Enter**.

   Note: If you are using a non-standard config file (for example, nc.test), substitute that config file name for nc.config.

   Result: A copy of the nc.config file (or the file name you specified), which contains configuration settings, is saved to a configuration file named nc.config.<_software version number>.
5. Remain logged in as root user and go to *Install Netcrypt Software onto the DNCS* (on page 9).

Install Netcrypt Software onto the DNCS

Introduction

This section describes how to install the new software onto the DNCS after downloading it from Cisco.com.

Create a Directory for the Software on the DNCS

Follow these instructions to create a directory on the DNCS. After the directory is created, you will download Netcrypt software from Cisco.com to this directory.

1. From the xterm window where you are logged in as root, type **cd /export/home/dncs/download** and press **Enter**. The /export/home/dncs/download directory becomes the working directory.

   Important: If this directory does *not* exist, use the **mkdir** command to create it. Then, repeat step 1.

2. Depending on the installation environment, type one of the following commands:

   - For a non-Overlay environment, type **mkdir NETCRYPT***xx* (where *xx* represents the software version number) and press **Enter**. The system creates a subdirectory called NETCRYPT in the /export/home/dncs/download directory.

     Example: If you are installing software version 1.2, type **mkdir NETCRYPT12**.

   - For an Overlay environment, type **mkdir NOBE***xx* (where *xx* represents the software version number) and press **Enter**. The system creates a subdirectory called NETCRYPT in the /export/home/dncs/download directory.

     Example: If you are installing software version 1.2, type **mkdir NOBE12**.

3 Depending on the installation environment, type one of the following commands:

- For a non-Overlay environment, type **cd NETCRYPT***xx* (where *xx* represents the software version number) and press **Enter** to access the NETCRYPT directory.

  Example: If you are installing software version 1.2, type **cd NETCRYPT12**.

- For an Overlay environment, type **cd NOBE***xx* (where *xx* represents the software version number) and press **Enter** to access the NOBE directory.

  Example: If you are installing software version 1.2, type **cd NOBE12**.

4 Go to ***Download the Software from Cisco*** (on page 10).

Download the Software from Cisco

Follow these instructions to download Netcrypt software. If you encounter any issues, contact your account representative for assistance.

1 From a web browser, navigate to Cisco.com.

2 Select **Support**.

3 Select Downloads.

4 In the Find field, enter one of the following terms and click **Find**:

- For non-Overlay environments, type **Netcrypt**.
- For Overlay environments, type **NOBE**.

5 From the Find results, click the software version you want to download and follow the prompts to download the software.

6 Go to ***Decompress and Extract the Software File*** (on page 10).

Decompress and Extract the Software File

1 From the xterm window, type one of the following commands that is appropriate for your installation environment:

- For non-Overlay environments, type **gzip -d NETCRYPT_***xx***.tar.gz** (where *xx* represents the software version number) and press **Enter**. The system decompresses the software file.

  Example: If you are installing Netcrypt software version 1.2, type **gzip -d NETCRYPT_12.tar.gz**.

- For Overlay environments, type **gzip -d NOBE_***xx***.tar.gz** (where xx represents the software version number) and press **Enter**. The system decompresses the software file.

  Example: If you are installing Netcrypt software version 1.2, type **gzip -d NOBE_12.tar.gz**.

2 Depending on the installation environment, type one of the following commands:

- For non-Overlay environments, type **tar xvf NETCRYPT_*xx*.tar** (where *xx* represents the software version number) and press **Enter**. The system extracts the individual files.

  Example: If you are installing Netcrypt software version 1.2, type **tar xvf NETCRYPT_12.tar**.

- For Overlay environments, type **tar xvf NOBE_*xx*.tar** (where *xx* represents the software version number) and press Enter. The system extracts the individual files.

  Example: If you are installing Netcrypt software version 1.2, type **tar xvf NOBE_12.tar**.

3 Go to ***Install the Software*** (on page 11).

Install the Software

1 From the xterm window where you are logged in as root, type **/usr/sbin/install_pkg** and press **Enter**.

Results:

- The system lists the packages that will be installed.
- A confirmation message appears asking you to confirm that you want to proceed with the installation.

2 Type **y** and press **Enter** to start the installation.

Note: The installation should take less than 30 seconds.

3 Did a message appear indicating that the installation was successful?

- If **yes**, go to step 4.
- If **no**, contact Cisco Services.

4 Use the UNIX **rm -rf** command to remove the following file and directory:

- For non-Overlay environments:
  - NETCRYPT*xx*tar (file)
  - NETCRYPT*xx* (directory)

  Note: Where *xx* represents the software version number.

  Example: If you are installing software version 1.2, type **rm -rf NETCRYPT12 NETCRYPT12.tar** and press **Enter**.

- For Overlay environments:
  - NOBE xxtar (file)
  - NOBE xx (directory)

  Note: Where xx represents the software version number.

  Example: If you are installing software version 1.2, type **rm -rf NOBE12 NOBE12.tar** and press **Enter**.

5 Type **exit** and press **Enter** to log out as root user.

6 Type **exit** and press **Enter** to close the xterm window.

7 Go to *Establish a Download Sequence* (on page 13).

Establish a Download Sequence

Establishing a Sequence for Downloading Software onto Each Netcrypt Bulk Encryptor

The order in which you download new software onto Netcrypt Bulk Encryptors allows you to verify that the download is successful before proceeding. Follow these guidelines to establish an order in which to download the new software to Netcrypt Bulk Encryptors. The method that you follow depends on the type of sessions that the Netcrypt Bulk Encryptor encrypts (xOD/VOD sessions or broadcast sessions).

CAUTION:

If you are upgrading more than one Netcrypt Bulk Encryptor, download the new software to one group of devices (for example, all of the devices in a single rack or hub) and verify the functionality before attempting to download the software to another group of devices. Verifying the functionality of one group of devices at a time enables you to better isolate any failures that may occur and enables you to minimize service interruptions.

xOD/VOD Sessions

When upgrading Netcrypt Bulk Encryptors that encrypt xOD or VOD sessions, we suggest that you upgrade all Netcrypt Bulk Encryptors in one hub and verify the functionality of those units before upgrading units in another hub.

Use the following guidelines to determine the order in which to upgrade Netcrypt Bulk Encryptors within a hub:

1. If any Netcrypt Bulk Encryptors act as spares, download the software on these units first.
2. If your system does not have a spare Netcrypt Bulk Encryptor, download the software on the unit carrying the fewest number of sessions.
3. Continue downloading the software to Netcrypt Bulk Encryptors by working your way up to the unit carrying the most sessions.

Broadcast Sessions

When upgrading Netcrypt Bulk Encryptors that encrypt broadcast sessions, upgrade the bulk encryptors in one hub, four bulk encryptors at a time, and verify their functionality before proceeding to other Netcrypt Bulk Encryptors in the hub.

Use the following guidelines to determine the order in which to upgrade Netcrypt Bulk Encryptors:

1. If any Netcrypt Bulk Encryptors act as spares, download the software on these bulk encryptors first.
2. If your system does not have a spare Netcrypt Bulk Encryptor, download the software on the bulk encryptor carrying sessions that are least viewed.
3. If you have Netcrypt Bulk Encryptors that carry BFS sessions, download the software to the BFS Netcrypt Bulk Encryptor first.
4. Continue downloading the software to bulk encryptors in this hub by working your way up to the bulk encryptor carrying sessions that are most frequently viewed.

What's Next?

You are ready to begin downloading the new software to the Netcrypt Bulk Encryptors. Go to ***Download Software to the Netcrypt Bulk Encryptors*** (on page 16).

2

Upgrading the Software

Introduction

This chapter describes how to upgrade software on the Netcrypt Bulk Encryptor.

In This Chapter

Download Software to the Netcrypt Bulk Encryptors

Introduction

To download the new software to Netcrypt Bulk Encryptors, you must first reset (reboot) the units by using one of the following methods:

- DNCS Administrative Console
- POWER switch on the back panel of the unit

> **CAUTION:**
>
> **All active sessions on the Netcrypt Bulk Encryptor will be interrupted when the bulk encryptor is reset. DHCTs downstream of the bulk encryptor will lose their ability to display services until sessions are reestablished.**

Important: Use ***Preparing to Monitor Remote Netcrypt Bulk Encryptor Resets*** (on page 16) when resetting Netcrypt Bulk Encryptors from the DNCS Administrative console.

After the bulk encryptors reset, the software is downloaded from the DNCS to the bulk encryptors and existing sessions are reestablished.

Choose a Reset Method

Choose one of the following methods to reset your Netcrypt Bulk Encryptors:

- To reset bulk encryptors through the DNCS Administrative Console, go to ***Preparing to Monitor Remote Netcrypt Bulk Encryptor Resets*** (on page 16).
- To reset bulk encryptors through the POWER switch, go to ***Physically Resetting the Netcrypt Bulk Encryptor*** (on page 18).

Preparing to Monitor Remote Netcrypt Bulk Encryptor Resets

1. From the xterm window, type **cd /dvs/dncs/tmp** and press **Enter** to access the TMP directory.
2. Type **ls -ltr boot*** and press **Enter**. A list of files starting with "boot" appears in the xterm window.
3. Locate the current bootpd.xxx file name.

   Note: This will be the bootpd.xxx file with the highest number and/or the most recent date.
4. Type **tail -f bootpd.xxx | grep -i netcrypt** to show the last Netcrypt Bulk Encryptor to reboot.

5 As you reset Netcrypt Bulk Encryptors from the Netcrypt List window, monitor the bootpd file to verify that each Netcrypt Bulk Encryptor reset.

Note: The bootpd file will roll over to the next log as it grows. If logging stops, repeat steps 2 through 4 to see if a new log file is being used.

6 Go to ***Resetting the Netcrypt Bulk Encryptor from the DNCS Administrative Console*** (on page 17).

Resetting the Netcrypt Bulk Encryptor from the DNCS Administrative Console

This section describes how to reset Netcrypt Bulk Encryptors in order to load new software. Use the ***Preparing to Monitor Remote Netcrypt Bulk Encryptor Resets*** (on page 16) procedure before resetting Netcrypt Bulk Encryptors from the DNCS Administrative Console.

CAUTION:

All active sessions on the Netcrypt Bulk Encryptor will be interrupted when the bulk encryptor is reset. DHCTs downstream of the bulk encryptor will lose their ability to display services until sessions are reestablished.

1 If you have not already done so, provision the bulk encryptor on the DNCS.

Note: For instructions to provision the Netcrypt Bulk Encryptor, refer to the appropriate guide: *Netcrypt Bulk Encryptor Hardware Installation and Operation Guide* (part number 4001444) or *Netcrypt Overlay Bulk Encryptor Installation and Operation Guide* (part number 4012215).

2 From the DNCS Administrative Console, click the **DNCS** tab, click the **Network Element Provisioning** tab, and then click **Netcrypt**. The Netcrypt List window opens.

3 Based on the order you determined earlier, select the Netcrypt Bulk Encryptor that you want to reset.

4 Click **Reset Selected**. The Question window opens and asks you to confirm the reset of the Netcrypt Bulk Encryptor.

5 Click **OK**. The Netcrypt List window displays a message to let you know that a request was received to reset the Netcrypt Bulk Encryptor.
Note: It may take up to 5 minutes for each Netcrypt Bulk Encryptor to reset.

6 Do you see the IP address for the Netcrypt you reset in the bootpd log file?

- If **yes**, continue with this procedure.
- If **no**, call Cisco Services.

Note: For details about IP addresses in the bootpd log file, go to ***Preparing to Monitor Remote Netcrypt Bulk Encryptor Resets*** (on page 16).

7 Repeat steps 3 through 6 for up to three additional bulk encryptors and then go to step 8.

Important: Never reset more than four bulk encryptors at once or you may cause bulk encryptors to retry downloads due to traffic congestion on the network.

8 Choose one of the following options and then go to step 9 of this procedure.

- For Netcrypt Bulk Encryptors that carry broadcast sessions, go to ***Verifying the Functionality of Modulators That Carry Netcrypt-Encrypted Broadcast Sessions*** (on page 18).
- For Netcrypt Bulk Encryptors that carry xOD or VOD sessions, go to ***Verifying the Functionality of Modulators That Carry Netcrypt-Encrypted xOD or VOD Sessions*** (on page 19).

9 Do you have additional bulk encryptors to reset?

- If **yes**, repeat steps 3 through 8.
- If **no,** go to step 10.

10 Click **Exit** to close the Netcrypt List window.

Physically Resetting the Netcrypt Bulk Encryptor

1 Reset the Netcrypt Bulk Encryptor by turning off and then back on the POWER switch located on the rear panel.

2 Repeat step 1 for up to three additional bulk encryptors.

Important: Never reset more than four bulk encryptors at once, or you may overload the DNCS.

3 Do you have additional Netcrypt Bulk Encryptors to reset?

- If **yes**, repeat steps 1 through 2 until each bulk encryptor has been reset, and then go to ***Verifying the Functionality of Modulators That Carry Netcrypt-Encrypted Broadcast Sessions*** (on page 18).
- If **no**, go to ***Verifying the Functionality of Modulators That Carry Netcrypt-Encrypted xOD or VOD Sessions*** (on page 19).

Verifying the Functionality of Modulators That Carry Netcrypt-Encrypted Broadcast Sessions

1 Access a DHCT that is connected downstream to one Netcrypt Bulk Encryptor.

2 Tune the DHCT to each channel that uses a source from a Netcrypt Bulk Encryptor that you reset and upgraded.

3 Are all channels for the Netcrypt Bulk Encryptors that you reset accessible from the DHCT?

- If **yes**, go to step 4.
- If **no**, do *not* attempt to upgrade the software for any additional Netcrypt Bulk Encryptors. Call Cisco Services at 1-800-283-2636.

4 For those Netcrypt Bulk Encryptors that carry content inappropriate for children, we recommend that you verify encryption using one of the following methods:

- Using a set-top that is authorized for all services, tune one-by-one to each service and check the PowerKEY Information diagnostic screen (page 6). If the Prog Stat and Prog Entitle fields are zero (0x00), then the program is in the clear. If these fields are non-zero, then the program is encrypted.
- Using a QAM tuner television, tune to the respective channels and verify that inappropriate content is not viewable.

5 Have you completed resetting your Netcrypt Bulk Encryptors?

- If **yes**, go to step 6.
- If **no,** return to the procedure you are using to reset your Netcrypt Bulk Encryptors.

6 Generate a Doctor Report using the **–av** option to verify system stability and functionality.

Note: For further instructions on running the Doctor Report, refer to the chapter titled **Analyze System Configuration With the Doctor Report** in the *DBDS Utilities Installation Instructions and DNCS Utilities User's Guide*. (Refer to the Netcrypt software release notes for the version of DBDS Utilities to use with the version of software that you are installing.)

7 Do new or unexpected errors appear in the Doctor Report?

- If **yes**, contact Cisco Services.
- If **no**, go to step 8.

8 Perform the System Validation Tests found in the installation and upgrade documentation for your system release version to verify the functionality and performance of the set-tops in your system.

9 Over the next few days, check the individual modulators that receive Netcrypt-encrypted sessions to verify that they are functioning as expected.

Verifying the Functionality of Modulators That Carry Netcrypt-Encrypted xOD or VOD Sessions

Important: Use the following procedure only when installing software in a non-Overlay environment. This procedure does not apply to installations performed in an Overlay environment.

Sessions that exist on xOD or VOD Netcrypt Bulk Encryptors that were upgraded will be interrupted and, in most cases, will recover. If the sessions do not recover, choose one of the following options:

1 Exit the xOD or VOD application (stop the xOD or VOD program), and then restart the application and the xOD or VOD stream by resuming the playback of the “in progress” purchase.

2 Change to a different channel, and then back to the previous channel. Restart the application and the xOD or VOD stream by resuming the playback of the "in progress" purchase.

Note: This procedure will vary depending on the application you are using.

Important: Due to load balancing and traffic, it is difficult to determine if all Netcrypt Bulk Encryptors are functioning properly. For this reason, you should monitor these units for a few days following this upgrade to verify that Session and Program Counts are increasing and/or decreasing (whichever is applicable) as new xOD or VOD sessions are created.

Note: After the upgrade is complete, perform the System Validation Tests found in the installation and upgrade documentation for your system release version to verify the functionality and performance of the set-tops in your system. If new or unexpected errors occur, contact Cisco Services.

3

Customer Information

If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.

A

Verify the Install Package Exists on the DNCS

Introduction

For system releases that do not include the pre-packaged install tool, we recommend that you verify whether or not the tool exists on your DNCS; because, the tool is required to load new software onto the DNCS. This appendix provides procedures for checking for the install tool, as well as procedures for retrieving it from Cisco.com.

In This Appendix

Check for the Install Tool on the DNCS

Checking for install_pkg on the DNCS

1. From an xterm window, type **cd /usr/sbin** and press **Enter**.
2. Type **ls** and press **Enter**.
3. Is the install_pkg file present on the DNCS?
   - If **yes**, resume your installation procedures.
   - If **no**, go to step 4.
4. From a web browser, navigate to Cisco.com.
5. Select **Support**.
6. Select Downloads.
7. In the Find field, enter one of the following terms and click **Find**:
   - For non-Overlay environments, type **Netcrypt**.
   - For Overlay environments, type **NOBE**.
8. From the Find results, click the software version you want to download and follow the prompts to download the software.

B

Load Multiple Versions of Netcrypt Code

The recommended upgrade process for Netcrypt Bulk Encryptors is based on a goal of getting all the units upgraded within a short period of time (typically one day). In some cases, a site may choose to upgrade the Netcrypt Bulk Encryptors over time or may desire to load a unique version of code onto a single Netcrypt Bulk Encryptor for extended testing. This appendix describes how to accomplish either of these goals.

In This Appendix

Loading Multiple Versions of Netcrypt Code

Note: If you need to determine which config files are being used by each Netcrypt Bulk Encryptor, refer to ***Checking for Multiple config Files*** (on page 5) for details. This procedure assumes that in a non-Overlay environment nc.config is the current configuration file, and in an Overlay environment, nobe.config is the current configuration file.

1. Go to the /tftpboot directory on the DNCS and rename the current software configuration file as **nc.current** or **nobe.current**, depending on your installation environment.
2. Install the new version of Netcrypt software that you intend to use by completing the steps in ***Install Netcrypt Software onto the DNCS*** (on page 9).
3. From the /tftpboot directory on the DNCS, rename the new software configuration file as **nc.new** or **nobe.new**, depending on your installation environment.
4. From the /tftpboot directory on the DNCS, rename the original backup file (for example, non-Overlay environments would rename **nc.current** to **nc.config** and Overlay environments would rename **nobe.current** to **nobe.config**).
5. From the Netcrypt List window on the DNCS, select the Netcrypt Bulk Encryptor that should download the new code and click **Open**. The Update Netcrypt window opens for this Netcrypt Bulk Encryptor.
6. Change the text in the **Configuration File** field according to the installation environment:
   - For non-Overlay environments, change the text from nc.config to **nc.new**.
   - For Overlay environments, change the text from nobe.config to **nobe.new**.
7. Click **Save**. The DNCS saves your change and displays the Netcrypt List window.
8. Select the Netcrypt Bulk Encryptor to which you want to download the new code and click **Reset**.
9. Repeat steps 5 to 8 for each Netcrypt Bulk Encryptor that you want to download the new code.

10 When you are ready to load code to all of your Netcrypt Bulk Encryptors, perform one of the following sets of steps:

- **Preferred Approach**
  - **i** Go to the /tftpboot directory and rename nc.new as **nc.config**. or **nobe.config**, depending on your installation environment.
  - **ii** From the Netcrypt List window on the DNCS, reset all the Netcrypt Bulk Encryptors that are using the nc.config or nobe.config file.
  - **iii** From the Update Netcrypt Element windows, change the configuration file value for all Netcrypt Bulk Encryptors that currently use nc.new or nobe.new to **nc.config** or **nobe.config**. These units do not need to be reset.
- **Alternative Approach**
  - **i** From the Update Netcrypt Element window, change the configuration file value for all units using nc.config or nobe.config to use **nc.new** or **nobe.new**.
  - **ii** Reset the changed Netcrypt Bulk Encryptors.

    Note: Units that were already using nc.new or nobe.new as their configuration file do not need to be reset.

C

Roll Back to the Previous Version of Netcrypt Software

This appendix contains instructions for restoring the previous version of Netcrypt software should you encounter problems after upgrading the software. Follow the instructions in this appendix only after Cisco Services directs you to restore the previous version of software.

Important: If after downloading software to the Netcrypt Bulk Encryptor, you encounter problems, contact Cisco Services at 1-800-283-2636 for assistance. In the event that Cisco Services directs you to download the previous version of software to Netcrypt Bulk Encryptors, follow the procedures in this appendix while working with Cisco Services.

In This Appendix

Introduction

Contact Cisco Services if you notice that the system is reacting adversely after installing or upgrading the Netcrypt software. If Cisco Services recommends restoring the previous Netcrypt software version, use the instructions in this section to assist you.

CAUTION:

Contact Cisco Services at 1-800-283-2636 before attempting to restore the previous Netcrypt software version.

Restore the Previous Version of Netcrypt Software

Note: To restore the previous Netcrypt executable files, restore the configuration backup file that you saved in ***Backing Up the Current Netcrypt or NOBE Configuration File*** (on page 8).

The procedure that you follow depends on the installation environment:

- For non-Overlay environments, go to ***Restoring the Previous Software Version in a Non-Overlay Environment*** (on page 31).
- For Overlay environments, go to ***Restoring the Previous Software Version in an Overlay Environment*** (on page 32).

Restoring the Previous Software Version in a Non-Overlay Environment

1. Open an xterm window on the DNCS and log on as the **root** user. The root prompt appears.
2. Type **cd /tftpboot** and press **Enter**. The root prompt appears.
3. Type **pwd** and press **Enter**. The text /tftpboot appears at the prompt. This text indicates you are in the correct directory.
4. Type **cp –p nc.config nc.config.***xx* (where *xx* represents the software version number) and press **Enter**. The configuration file named nc.config, which contains Netcrypt version 1.0 configuration settings, is saved to a file named nc.config.xx.

   Example: If software version 1.2 is currently installed on the Netcrypt, you would type **cp -p nc.config nc.config12** and press **Enter**. As a result, the configuration file that is currently installed on the Netcrypt would be saved to a file named nc.config.12.
5. Type **cp –p nc.config.<software version number> nc.config** and press **Enter.** The configuration file named nc.config.old, which contains the previous list of Netcrypt configuration files, is copied to a configuration file named nc.config.
6. Type **ls -l** and press **Enter**. A list of files displays. The files **nc.config.<software version number>**, **nc.config**, and **nc.config.xx** appear in the list.

   Note: The "l" used in **ls** and **-l** is a lowercase letter L.
7. Confirm that the date and size of **nc.config** matches those of **nc.config.<software version number>**.
8. Type **exit** and press **Enter**.
9. Download the previous version of software to Netcrypt Bulk Encryptors by rebooting the units. For detailed procedures, go to ***Download Software to the Netcrypt Bulk Encryptors*** (on page 16).

Restoring the Previous Software Version in an Overlay Environment

1. Open an xterm window on the DNCS and log on as the **root** user. The root prompt appears.
2. Type **cd /tftpboot** and press **Enter**. The root prompt appears.
3. Type **pwd** and press **Enter**. The text /tftpboot appears at the prompt. This text indicates you are in the correct directory.
4. Type **cp –p nobe.config nobe.config.***xx* (where *xx* represents the software version number) and press **Enter**. The configuration file named nobe.config, which contains Netcrypt version 1.0 configuration settings, is saved to a file named nobe.config.xx.

   Example: If software version 1.2 is currently installed on the Netcrypt, you would type **cp -p nobe.config nobe.config12** and press **Enter**. As a result, the configuration file that is currently installed on the Netcrypt would be saved to a file named nobe.config.12.
5. Type **cp –p nobe.config.<software version number> nobe.config** and press **Enter.** The configuration file named nobe.config.old, which contains the previous list of Netcrypt configuration files, is copied to a configuration file named nc.config.
6. Type **ls -l** and press **Enter**. A list of files displays. The files **nobe.config.<software version number>**, **nobe.config**, and **nobe.config.xx** appear in the list.

   Note: The "l" used in **ls** and **-l** is a lowercase letter L.
7. Confirm that the date and size of **nobe.config** matches those of **nobe.config.<software version number>**.
8. Type **exit** and press **Enter**.
9. Download the previous version of software to Netcrypt Bulk Encryptors by rebooting the units. For detailed procedures, go to ***Download Software to the Netcrypt Bulk Encryptors*** (on page 16).

Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678 277-1120
800 722-2009
www.cisco.com

August 2012 Printed in United States of America Part Number 4021238 Rev C