Netcrypt Bulk Encryptor Software Version 1.1.3

Release Notes and 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. A listing of Cisco's trademarks can be found at **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. (1009R)

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 the information and procedures for installing Netcrypt™ software version 1.0 on a Netcrypt Bulk Encryptor. This document also provides a description of the functionality this software provides for a Netcrypt Bulk Encryptor.

Purpose

This document enables system operators to install Netcrypt software version 1.0 on a Netcrypt Bulk Encryptor.

Scope

This document provides instructions to install Netcrypt software version 1.0 on a Netcrypt Bulk Encryptor. It does not provide instructions for installing a Netcrypt Bulk Encryptor in your headend.

Note: For instructions to install a Netcrypt Bulk Encryptor in your headend, refer to *Netcrypt™ Bulk Encryptor Hardware Installation and Operation Guide.* For the part number for this document, see ***Related Publications*** (on page v).

Audience

System operators or Cisco engineers who are responsible for installing Netcrypt software onto a Netcrypt Bulk Encryptor should read this publication.

Related Publications

You may find the following publications useful as resources when you implement the procedures in this document. Check the copyright date on your resources to assure that you have the most current version. The publish dates for the following documents are valid as of this printing. However, some of these documents may have since been revised:

- *DBDS Utilities Version 6.1 Installation Instructions and DNCS Utilities User's Guide* (part number 740020, expected publish date: late 2006)
- *Netcrypt™ Bulk Encryptor Hardware Installation and Operation Guide* (part number 4001444, [revision expected date: late 2006])

Document Version

This is the second release of this document.

1

Introducing Netcrypt Software Version 1.1.3

Introduction

This chapter lists the requirements for upgrading the Netcrypt Bulk Encryptor with Netcrypt software version 1.1.3. This chapter also describes the functionality that Netcrypt software version 1.1.3 provides.

In This Chapter

About the Software

Netcrypt Bulk Encryptor software version 1.1.3 provides the following key features:

- Encrypts as many as 4000 input programs into a maximum of 4000 standard definition transport streams suitable for digital broadcast or multicast sessions.
- Provides multicasting support using Internet Group Management Protocol, Version 2 (IGMPv2).
- Offers a flexible design for broadcast and on-demand applications in systems that use MPEG transport over UDP, IP, and Ethernet.
- Provides status alarms to help you monitor and maintain a Netcrypt Bulk Encryptor. In addition, if Cisco's optional Alarm Management System is used, Netcrypt alarms can be monitored on the Digital Network Control System (DNCS).

Want to Learn More About Netcrypt Features?

For more information about a Netcrypt Bulk Encryptor, including theory of operation, refer to *Netcrypt™ Bulk Encryptor Hardware Installation and Operation Guide*. The guide also provides instructions for installing, provisioning, operating, and using alarms to troubleshoot a Netcrypt Bulk Encryptor. For the part number of the guide, see ***Related Publications*** (on page v).

What Are the Site Requirements?

This section provides information to help you prepare for upgrading a Netcrypt Bulk Encryptor with Netcrypt 1.1.3 . This section includes important information to help you schedule the appropriate amount of time for the upgrade. Please read this entire section before you upgrade to Netcrypt software version 1.1.3.

System Release Compatibility and Prerequisites

Netcrypt software can be installed on a DBDS that is running one of the following system releases:

- SR 2.7/SR 3.7 and later releases
- SR 4.2 and later releases

For a complete configuration listing, or to upgrade your system, contact Cisco Services.

Software

Netcrypt 1.1.3 includes the following software:

- Netcrypt Host Application code 1.1.3
- Netcrypt Host Boot code 1.1.3
- Netcrypt Input Application code 1.1.3
- Netcrypt Input Boot code 1.1.3
- Netcrypt Output Application code 1.1.3
- Netcrypt Output Boot code 1.1.3
- Field Programmable Gate Array (FPGA) code 16.8

Hardware

Netcrypt software version 1.1.3 supports only the Netcrypt Bulk Encryptor.

Known Issues

There are no known issues at the time of this release.

2

Upgrading the Software

Introduction

This chapter describes how to upgrade the Model D9477 Netcrypt with software version 1.1.3.

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 to Netcrypt 1.1.3, be sure that your system meets the criteria specified in ***System Release Compatibility and Prerequisites*** (on page 3) and Cisco Application Platform Release Dependencies.

If you will not be downloading the Netcrypt software from the Cisco File Transfer Protocol (FTP) site, make sure that you have obtained the CD, **Netcrypt Software V1.1.3**, part number 4017778.

Time to Complete

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

- Completing pre-upgrade tasks takes from 30 to 45 minutes.
- If you are upgrading from an FTP site, allow an additional 10 to 15 minutes to download the software from the FTP site. The speed of the connection and the size of the files will determine the actual download time.
- Downloading new software to the Netcrypt Bulk Encryptor takes approximately 5 minutes for each bulk encryptor.
- 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 that are determined to be active will be restarted. Because 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 encrypt are interrupted. DHCTs will show a frozen picture or "black screen" until the upgrade is complete and the DNCS has restarted all of the active sessions that the Netcrypt Bulk Encryptor encrypts.

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 21)
- ***Verifying the Functionality of Modulators that Carry Netcrypt-Encrypted xOD or VOD Sessions*** (on page 22)

Process Overview

This section provides an overview of the process required to upgrade to Netcrypt 1.1.3.

Important! You should only upgrade Netcrypt Bulk Encryptors 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 bulk encryptor group (for example, all bulk encryptors in a single rack or hub) and verify its functionality before attempting to download the software to another bulk encryptor group. Verifying the functionality of one bulk encryptor group 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 25).
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 configuration file.
5. If you are upgrading more than one Netcrypt Bulk Encryptor, establish an order for upgrading the bulk encryptors.

Install the Netcrypt software onto the DNCS from either the Cisco FTP site or a CD.

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 bulk encryptors you plan to upgrade. This will allow you to verify that these sessions are rebuilt after the new software is downloaded to the bulk encryptors.
3. Verify that the upgraded Netcrypt Bulk Encryptor is functioning properly.

   Important! Read and follow the directives contained in ***Impact of TVs with QAM Tuners*** (on page 7).
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 to Netcrypt 1.1.3, verify the number of configuration files in use and what Netcrypt 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 for the Netcrypt is **/tftpboot/nc.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.

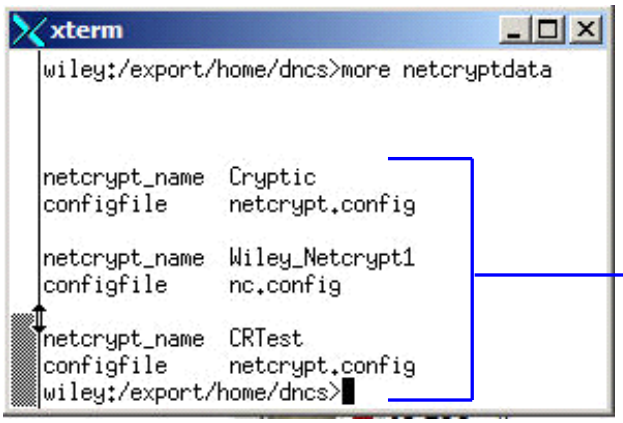
1. From the DNCS Administrative Console, click **Utilities** and click **xterm**. The xterm window opens.
2. Type **dbaccess dncsdb <<%** and press **Enter**.
3. Type **output to netcryptdata select netcrypt_name, configfile from netcrypt;** and press **Enter**.
4. Type % and press **Enter**. A result, 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 11).

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

- If **yes**, refer to ***Load Multiple Versions of Netcrypt Code*** (on page 27).
- 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 **Open Selected**. The Update Netcrypt window opens.

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

d Click **Update** to save this change.

9 Go to ***Checking the Software Version Associated with the config File*** (on page 11).

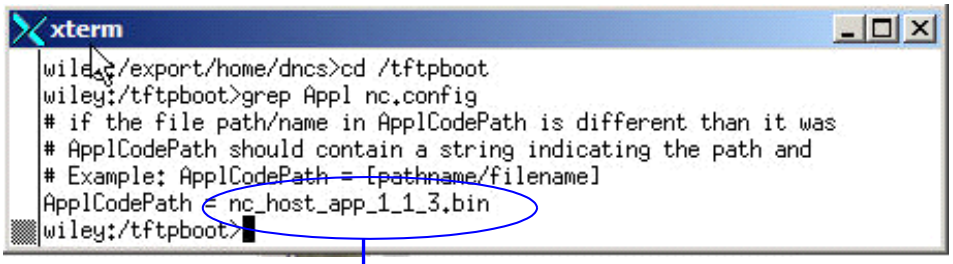
Checking the Software Version Associated with the config File

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 9), 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 12).

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 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. Copy the current configuration file to a backup file.

   Example: Type **cp –p nc.config nc.config.old** 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.old.
5. Remain logged in as root user and go to ***Install Netcrypt Software onto the DNCS*** (on page 13).

Install Netcrypt Software onto the DNCS

Introduction

This section describes how to install the new software onto the DNCS. Software is installed from either of the following locations:

- Netcrypt Software V1.1.3 CD, part number 4017778. Go to ***Installing the Netcrypt Software from a CD*** (on page 13).
- Cisco's FTP server. Go to ***Installing the Netcrypt Software from the Cisco FTP Server*** (on page 14).

Installing the Netcrypt Software from a CD

1. Insert the **Netcrypt Software V1.1.3** CD into the CD-ROM drive of the DNCS.
2. Did the File Manager window display?
   - If **yes**, the CD mounted successfully.
   - If **no**, type **df -k** to determine where the CD is mounted and then go to step 3.
3. Is /cdrom listed in the output?
   - If **yes**, go to step 4.
   - If **no**, contact Cisco Services.
4. From the xterm window where you are logged in as root, type **cd /cdrom/cdrom0** and press **Enter** to access the cdrom0 directory.
5. 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.
6. Type **y** and press **Enter** to start the installation. When the installation is complete, the system displays a message stating that the installation was successful and a prompt for the root user appears.

   Note: The installation should take less than 30 seconds.
7. Was the installation successful?
   - If **yes**, go to step 8.
   - If **no**, contact Cisco Services.
8. From the xterm window where you are logged in as root, type **exit** and press **Enter**. You are logged out as root user.

9 Complete one of the following steps:

   a **If the File Manager is present**: From the File Manager window, click **File** and select **Eject**. The CD is ejected from the CD drive and the File Manager window closes.

   b **If the File Manager is not present**: From an xterm window, type the following command: **cd /.; eject; exit**. The CD is ejected from the CD drive.

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

11 Go to *Establish a Download Sequence* (on page 16).

Installing the Netcrypt Software from the Cisco FTP Server

Creating the 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 Type **mkdir NETCRYPT113** and press **Enter**. The system creates a subdirectory called NETCRYPT113 in the /export/home/dncs/download directory.

3 Type **cd NETCRYPT113** and press **Enter** to access the NETCRYPT113 directory.

4 Go to *Obtaining the Netcrypt Software File* (on page 14).

Obtaining the Netcrypt Software File

1 Log on to the Cisco FTP server.

   Notes:

   - The address of the server is **ftp.sciatl.com** or **192.133.243.133**.

     Note: The address for the Cisco FTP server is subject to change. If you are unable to reach the FTP server, please contact Cisco Services for the latest address.

   - The username is **anonymous**.

   - The password is the email address of the person logging in.

2 Choose one of the following options to navigate to the directory in which the file is located:

   - If you are *outside* of Cisco's firewall, type **cd /pub/scicare/RELEASED/NETCRYPT**

   - If you are *inside* of Cisco's firewall, type **cd /external_pub/scicare/RELEASED/NETCRYPT**

3 Type **bin** and press **Enter**. The system sets the ftp transfer mode to binary.

4 Type **hash** and press **Enter**. The system configures itself to display hash marks that show file-transfer progress.

5 Type **prompt** and press **Enter**. The system indicates that interactive mode is off.

6 Type **mget** * and press **Enter**. The system begins copying the file (or files) from the FTP site to the current directory on your DNCS.

7 Type **bye** and press **Enter** to log out of the Cisco FTP server.

8 Go to ***Decompressing and Extracting the File*** (on page 15).

Decompressing and Extracting the File

1 From the xterm window, type **gzip -d NETCRYPT_1.1.3.tar.gz** and press **Enter**. The system decompresses the Netcrypt software file.

2 Type **tar xvf NETCRYPT_1.1.3.tar** and press **Enter**. The system extracts the individual files.

3 Go to Installing Netcrypt Software.

Installing Netcrypt 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 -rfi** command to remove the following file and directory:

- NETCRYPT113.tar (file)
- NETCRYPT113 (directory)

Example: Type **rm –rf NETCRYPT113 NETCRYPT113.tar** and press **Enter**.

Result: A confirmation question message appears asking you to confirm the removal.

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 16).

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 bulk encryptor group (for example, all bulk encryptors in a single rack or hub) and verify its functionality before attempting to download the software to another bulk encryptor group. Verifying the functionality of one bulk encryptor group 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 18).

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 18) 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 18).
- To reset bulk encryptors through the POWER switch, go to ***Physically Resetting the Netcrypt Bulk Encryptor*** (on page 20).

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 19).

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 18) 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 re-established.

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 *Netcrypt™ Bulk Encryptor Hardware Installation and Operation Guide*.

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 QAM 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 18).

7 Repeat steps 3 through 6 for up to three additional bulk encryptors and then go back 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 21).
- 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 22).

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 21).
- If **no**, go to ***Verifying the Functionality of Modulators That Carry Netcrypt-Encrypted xOD or VOD Sessions*** (on page 22).

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 5.
   - If **no**, do *not* attempt to upgrade the software for any additional Netcrypt Bulk Encryptors. Call Cisco Services.
4. For those Netcrypt Bulk Encryptors that carry content inappropriate for children, Cisco recommends 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 Version 6.1 Installation Instructions and DNCS Utilities User's Guide*.
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

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 the Scientific Atlanta FTP site.

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. Log on to the Scientific Atlanta FTP server.

   Notes:

   - The address of the server is **ftp.sciatl.com** or **192.133.243.133**.

     Note: The address for the Scientific Atlanta FTP server is subject to change. If you are unable to reach the FTP server, please contact Cisco Services for the latest address.
   - The username is **anonymous**.
   - The password is the email address of the person logging in.
5. Choose one of the following options to navigate to the directory in which the file is located:
   - If you are *outside* of Scientific Atlanta's firewall, type **cd /pub/scicare/RELEASED/NETCRYPT**
   - If you are *inside* of Scientific Atlanta's firewall, type **cd /external_pub/scicare/RELEASED/NETCRYPT**
6. Type **bin** and press **Enter**. The system sets the ftp transfer mode to binary.
7. Type **hash** and press **Enter**. The system configures itself to display hash marks that show file-transfer progress.
8. Type **prompt** and press **Enter**. The system indicates that interactive mode is off.
9. Type **mget** * and press **Enter**. The system begins copying the file (or files) from the FTP site to the current directory on your DNCS.
10. Type **bye** and press **Enter** to log out of the Scientific Atlanta FTP server.
11. Continue with the installation procedures.

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 9) for details. For this procedure, we will assume that nc.config is the current configuration file.

1. Go to the /tftpboot directory on the DNCS and rename the current nc.config file as **nc.current**.
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 13).
3. From the /tftpboot directory on the DNCS, rename the new nc.config file as **nc.new**.
4. From the /tftpboot directory on the DNCS, rename the original backup file (for example, rename nc.current to nc.config).
5. From the Netcrypt List window on the DNCS, select the Netcrypt Bulk Encryptor that should download the new code and click **Open Selected**. The Update Netcrypt Element window opens for this Netcrypt Bulk Encryptor.
6. Change the **Configuration File** field from nc.config to **nc.new**.
7. Click **Update**. 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 Selected**.
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**.
      ii. From the Netcrypt List window on the DNCS, reset all the Netcrypt Bulk Encryptors that are using the nc.config file.
      iii. From the Update Netcrypt Element windows, change the configuration file value for all Netcrypt Bulk Encryptors that currently use nc.new to **nc.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 to use **nc.new**.
      ii. Reset the changed Netcrypt Bulk Encryptors.

      Note: Units that were already using nc.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 to Netcrypt 1.1.3. Follow the instructions in this appendix only after Cisco Services directs you to restore the previous version of software.

Important! If after downloading Netcrypt 1.1.3 you encounter problems, contact Cisco Services for assistance. In the event that Cisco 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 to Netcrypt 1.1.3. If Cisco Services recommends restoring the previous Netcrypt software version, use the instructions in this section to assist you.

CAUTION:

Contact Cisco Services before attempting to restore the previous Netcrypt software version.

Restore the Previous Version of Netcrypt Software

Restoring the Previous Netcrypt Software Version

Note: To restore the previous Netcrypt executable files, restore the configuration backup file that you saved in ***Backing Up the Current Netcrypt Configuration File*** (on page 12).

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.yyy** and press **Enter**. The configuration file named nc.config, which contains Netcrypt version 1.1.3 configuration settings, is saved to a file named nc.config.yyy.

   Note: The yyy represents the Netcrypt software version number you just installed.
5. Type **cp –p nc.config.old 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.old**, **nc.config**, and **nc.config.bakyyy** 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.old**.
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 18).

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

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

June 2012 Printed in USA

Part Number 4009746 Rev B