DBDS Backup and Restore Procedures

For SR 2.2 and SR 3.2, SR 2.4 and SR 3.4, SR 2.5 and SR 3.5, and SR 3.3

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 Acknowledgments

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 v

Chapter 1 Release Notes
Overview 1-1
Implemented Change Requests 1-2

Chapter 2 Backup Recommendations
Overview 2-1
System Backup Recommendations 2-2
Tape Considerations 2-3

Chapter 3 Backing Up and Restoring the Informix Database
Overview 3-1
Back Up the Informix Database 3-2
Restore the Informix Database 3-8

Chapter 4 Backing Up and Restoring the DNCS and Application Server
Overview 4-1
Back Up the DNCS or Application Server File System 4-2
Back Up the DNCS or Application Server Key Files 4-7
Restore the DNCS or Application Server File System 4-11
Restore the DNCS or Application Server Key Files 4-19

Chapter 5 Customer Information 5-1

Appendix A Stopping System Components
Overview A-1
Stop System Components A-2

Appendix B Restarting System Components
Overview B-1
Restart System Components B-2

Appendix C Setting Up an Automated Database Backup
Overview C-1
Configure the DNCS for an Automatic Database Backup C-2

About This Guide

Purpose

This guide provides a full set of backup and restore procedures for Cisco's Digital Broadband Delivery System (DBDS) databases, as well as for the Digital Network Control System (DNCS) and the Cisco Application Server key files and file system.

Audience

These backup and restore procedures are written for operators of Cisco's DBDS who support System Release (SR) 2.2 or SR 3.2 (including all service packs), SR 2.4 or SR 3.4, SR 2.5 or SR 3.5, or SR 3.3.

Cisco field service engineers and software installers may also find the information in this guide useful as they assist system operators in installing, troubleshooting, and maintaining their systems.

Scope

The procedures in this guide for backing up and restoring the Application Server pertain only to Cisco Application Servers. System operators who support other application servers should contact their vendor for relevant backup and restore procedures.

DBDS Maintenance CD

Be sure that you have version 2.0.x of the DBDS Maintenance CD before starting any of the backup or restore procedures covered in this guide. Version 2.0.x of the DBDS Maintenance CD contains all the scripts needed to back up and restore your system.

Document Version

This is the second release of these backup and restore procedures.

Chapter 1
Release Notes

Overview

Introduction

This chapter lists those change requests (CRs) that were implemented during the development and testing of the backup and restore procedures covered in this guide, as well as the hardware platforms with which the backup and restore scripts are compatible.

Hardware Platform Compatibility

Version 6.0.x of the backup and restore scripts, which is a part of the DBDS Maintenance CD 2.0.x, was tested against the following platforms:

- DNCS
  - Sun Enterprise 250
  - Sun Enterprise 450
  - Sun Fire V880
- Application Server
  - Sun Blade 150
  - Sun Ultra 2
  - Sun Ultra 5

For a complete configuration listing for the System Releases, please contact Cisco Services.

In This Chapter

This chapter contains the following topic.

Topic	See Page
Implemented Change Requests	1-2

Implemented Change Requests

Introduction

This section provides information about the CRs that were implemented during development of the SR 2.2 and SR 3.2, SR 2.4 and SR 3.4, SR 2.5 and SR 3.5, and SR 3.3 backup and restore procedures. The CRs are presented in quick-reference format, as well as in a format that provides a more detailed description.

Note: If you need additional information about the CRs, please contact Cisco Services.

Quick Reference to Implemented CRs

This section contains a quick reference to the CRs implemented during the release of the backup and restore procedures covered in this guide.

CR Number	Short Description
36770	The dncsFilesBackup script now supports file names that exceed 100 characters in length.
38394	The restoreFileSystems script now builds Sun Fire 880 devices correctly.
41007	The inaccurate timestamp assigned to the key files restoration process has been corrected.

Detailed Descriptions of Implemented CRs

This section contains detailed descriptions of the CRs implemented during the release of the backup and restore procedures covered in this guide.

File Names Exceeding 100 Characters Supported

The dncsFilesBackup script has been modified so that it now supports file names that exceed 100 characters in length. CR **36770** addresses this issue.

Sun Fire 880 Devices Build Correctly

The restoreFileSystems script has been modified so that it now builds files in the /devices, /dev/dsk, and /etc/path_to_inst directories correctly. CR **38394** addresses this issue.

Timestamp of Key Files Restoration Process is Now Assigned Correctly

Cisco engineers have devised a workaround to a system error that assigned an incorrect timestamp to the key files restoration process. CR **41007** addresses this issue.

Chapter 2
Backup Recommendations

Overview

Introduction

This chapter provides recommendations for the frequency with which system operators should back up the data of their Digital Broadband Delivery System (DBDS). By performing regular backups, system operators are assured that their valuable data will not be lost should they ever experience a failure of a major component of their DBDS system.

System operators can back up their data to either 4-mm data tapes or 8-mm data tapes, depending upon the type of tape drive installed in their DNCS or Application Server. Use the information in this chapter for tape selection and tape cleaning recommendations.

In This Chapter

This chapter contains the following topics.

Topic	See Page
System Backup Recommendations	2-2
Tape Considerations	2-3

System Backup Recommendations

Introduction

Cisco recommends that system operators perform a complete system backup (file systems and database) prior to making any substantial modification to the system. System operators can ensure the integrity of their DBDS data only by adhering to a regular schedule of database and file system backups. The recommendations in this section provide some guidance regarding the frequency with which system backups should occur. Adjust these recommendations, if necessary, according to the size of the system and the frequency with which the data changes.

Informix Database Backups

The Informix database on the DNCS contains all headend configuration information, as well as data needed to provision and authorize Digital Home Communication Terminals (DHCTs). Cisco recommends that system operators perform a complete backup of the Informix database once a day. In addition, Cisco recommends that system operators perform a complete backup of the database immediately before and after a channel lineup change or a major system configuration change. Use the procedures in this guide to back up the Informix database.

Note: Refer to Appendix C, **Setting Up an Automated Database Backup**, for a procedure that sets up an automatic database backup. You can use this procedure if your database backup requires only one tape.

File System Backups

Cisco recommends that system operators perform a complete backup of the DNCS and Application Server file systems at a minimum of once a month.

Important: Beginning with SR 2.2 and SR 3.2, you can now back up the file system of the DNCS and the Application Server without first shutting down the system components. Even though you are no longer required to shut down the system components, Cisco highly recommends that you schedule your file system backups for periods of lowest system activity.

Complete System Backups

Cisco recommends that system operators perform a complete system backup just prior to upgrading to new system software, as well as after the upgrade. This backup will be used in case the system must be rolled back to the previous release in the event that the upgrade is unsuccessful.

Important: Clearly label the backup and remove it from the working area so that it cannot be accidentally restored to the new release. New and old backups are not compatible.

Tape Considerations

Two Types of Tape

Consider the following issues when selecting the type of tapes to buy for the backups:

- You can back up your files to either a 4-mm or an 8-mm data tape. The type of tape you choose depends upon the type of tape drive installed on your DNCS or Application Server.
- You can purchase 4-mm tapes or 8-mm tapes in various lengths. Refer to the following chart, compiled by Cisco engineers, for the specifications of the various tapes available for use in your tape drives.

Tape Drive	Tape Length (in meters)	Capacity (normal/compressed) (in Gbytes)	Tapesize (in Kbytes)	Blocksize (in Kbytes)
8 mm	54	2/4	3774874	16
8 mm	112	5/10	9437184	32
8 mm	160	7/14	13212058	128
4 mm	90	2/4	3774874	16
4 mm	120	4/8	7549747	32
4 mm	125	12/24	22649242	128
4-mm	150	20/40	36864000	128

- The rows shaded in gray represent Cisco's recommendations.
  - If you use an 8-mm tape drive, buy tapes that are 160 meters long.
  - If you use a 4-mm tape drive, buy tapes that are 125 meters long.
- Depending upon the size of your database, you may need more than one tape to do a complete database backup. If you need more than one tape to back up your database, the backup and restore scripts will prompt you to remove the existing tape and to insert a new tape at the appropriate time.

Cleaning Your Tape Drive

Under normal conditions, most tape and tape drive manufacturers recommend that you clean your tape drive after about 30 hours of data transfer. Use only a cleaning cartridge and kit designed for use with your tape drive. Discard your cleaning cartridge after using it for the number of cleaning cycles specified in the cleaning kit documentation.

Chapter 3
Backing Up and Restoring the Informix Database

Overview

Introduction

The Informix database on the DNCS contains all headend configuration information, as well as data needed to provision and authorize DHCTs. Cisco recommends that you back up your Informix database once a day.

Some large systems require more than one tape when backing up the database. The backup script prompts you to insert another tape at the appropriate time if your backup requires an additional tape.

Use seven tapes (or seven sets of tapes), one for each day of the week, when you back up your database.

Note: You do not have to shut down the DNCS or the Application Server in order to back up your Informix database. All system components can be running while you back up the database.

When to Back Up the Database

Cisco recommends that you back up your Informix database early in the morning or late at night, when system activity is usually at a minimum.

Back up your database *before* your billing system uploads subscriber impulse pay-per-view (IPPV) purchases from your DNCS. By backing up your database *before* your billing system uploads IPPV purchases, you have a record of subscriber purchases in the event that the billing system loses this data.

Avoid backing up your database while you are performing the following system tasks:

- Running the Interactive Program Guide (IPG) Collector
- Loading an Entitlement Management Message (EMM) CD
- Staging DHCTs
- Downloading IPPV events

In This Chapter

This chapter contains the following topics.

Topic	See Page
Back Up the Informix Database	3-2
Restore the Informix Database	3-8

Back Up the Informix Database

Introduction

This section contains the following information:

- Default DNCS tape drive configuration information
- A procedure to determine the configuration of the tape drive in use on your system
- Procedures to back up the Informix database

Default Tape Drive Configuration

The script used by the DNCS to back up the Informix database uses the following default tape drive configuration:

- Tape size: 7549747 KB
- Block size: 32 KB
- Device name: /dev/rmt/0h

This tape drive configuration is in use on a majority of systems. Occasionally, however, the tape drive on a system may be configured with a different device name, such as /dev/rmt/1h.

Note: The 'h' that appears at the end of device name /dev/rmt/0h or /dev/rmt/1h indicates that the system is to use a high density format (compressed) when writing to the tape.

If you know that the device name of your tape drive is /dev/rmt/0h, you may skip the following procedure, **Checking Your Tape Drive Configuration**, and continue with **Backing Up the Informix Database**, later in this section. However, if you are unsure of the device name of your tape drive, or if you just want to verify that the device name is /dev/rmt/0h, complete the following procedure.

Checking Your Tape Drive Configuration

Use this procedure if you need to determine the device name of the tape drive used by your DNCS.

Notes:

- You will only have to complete this procedure once. The device name of your tape drive will not change unless you specifically change the tape drive configuration.
- Do not have a tape in the tape drive when you complete this procedure.

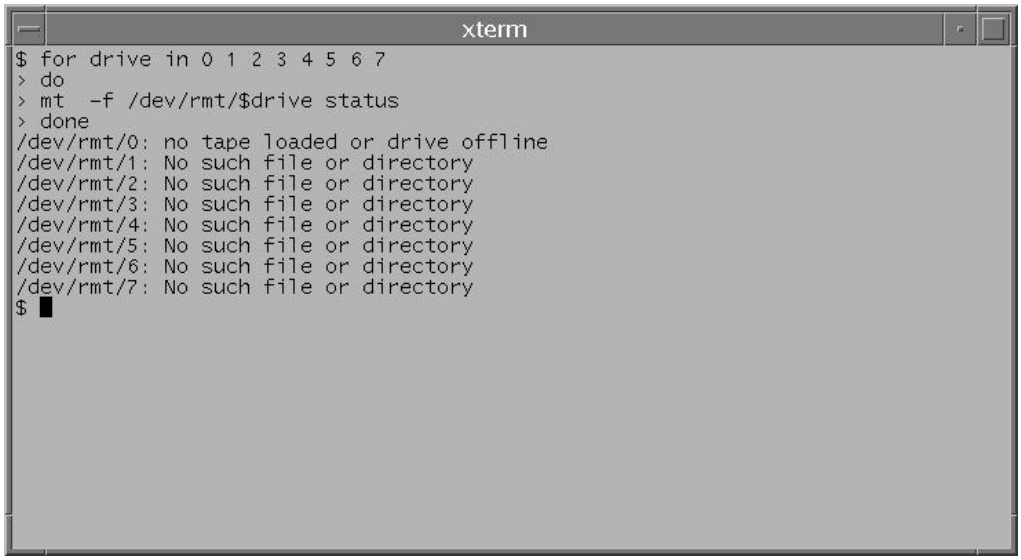
1. If necessary, open an xterm window on the DNCS.
2. Ensure that no tape is currently in your tape drive.
3. Type the following UNIX routine.

   Important: Type the routine just as shown by pressing **Enter** at the end of each line.

   ```
   for drive in 0 1 2 3 4 5 6 7
   do
   mt  -f  /dev/rmt/$drive status
   done
   ```

   Result: The system checks the status of eight possible tape drive configurations and displays the results.

   Note: Your system will display results similar to the following illustration.



4. Examine your results and use the following observations, based upon the example used in step 3, to determine the device name of your tape drive.
   - In the example in step 3, no tape drives are detected in **/dev/rmt/1** through **/dev/rmt/7** (as indicated by *No such file or directory*). Therefore, you can conclude that /dev/rmt/1 through /dev/rmt/7 are not valid device names for tape drives on the system queried in step 3.
   - In the example in step 3, a tape drive is detected in **/dev/rmt/0** and the system accurately notes that no tape is loaded. Therefore, you can conclude that the device name of the tape drive on the system queried in step 3 is /dev/rmt/0.
   - If /dev/rmt/1 is the device name of your tape drive, then *no tape loaded or drive offline* would appear next to /dev/rmt/1.
5. Write the device name of your tape drive in the space provided.

   _____

   Note: You may need to refer to this device name in a leter procedure, **Backing Up the Informix Database**, or **Restoring the Informix Database**.

Database Backup Script Options

The script that backs up the databases is called **backupDatabase**. You can run the backupDatabase script with the following options:

- *-b* — TAPEBLK. Specifies the block size of the tape device to which ontape writes during the database backup.

  Note: The system uses a default tape block size of 32 if *–b* is not specified.
- -s – TAPESIZE. Specifies the size of the tape device to which ontape writes during the database backup.

  Note: The system uses a default tape size of 7549747 if *–s* is not specified.
- *-l* — local-tape-drive. Specifies tape drive to use on local host. (e.g. -- /dev/rmt/0h)
- -r – remote-tape-drive. Specifies tape drive on a remote host. (e.g. – sparky: /dev/rmt/0h or 192.168.1.10: /dev/rmt/0h)
- *-check-database* — Checks the integrity of the databases. (Does not fix if errors are found.)
- *-non-interactive* — Non-interactive, useful when running from cron.
- *-verbose* — Verbose output.

Backing Up the Informix Database

Use this procedure to back up the Informix database.

Notes:

- The DNCS, the Application Server, and Spectrum can be running while you back up the Informix database.
- It may take up to 30 minutes to back up a typical database with approximately 100,000 DHCTs.

1. If necessary, open an xterm window on the DNCS.
2. Type **su -** and then press **Enter** to log in as root user.

   Note: Be sure to type the single dash after typing su.

   Result: The **password** prompt appears.
3. Type the root password and then press **Enter**.
4. Insert the CD labeled **DBDS Maintenance CD 2.0.x** into the CD drive of the DNCS.
5. Type **df -n** and then press **Enter**.

   Result: A list of the mounted filesystems appears.

   Note: The presence of **/cdrom** in the output confirms that the system correctly mounted the CD.
6. Label your backup tape with the following information:

   DNCS Database Backup [Day of the Week]
   [Site Name]
   [Software Version]
   DBDS Maintenance CD 2.0.x
   [Tape #]

   Notes:

   - Customize the label with the day of the week, site name, and software version for the site you are backing up.
   - If your database backup requires more than one tape, be sure to note the tape number on the label.
7. Insert the tape into the tape drive of the DNCS and wait until the green light stops flashing.

   Important: Be sure that you are using different tapes for each day of the week, as recommended in the **Introduction** to this chapter.

8. Type **. /dvs/dncs/bin/dncsSetup** and then press **Enter**.

   Important: Be sure to type the dot prior to typing /dvs.

   Result: The system establishes the root user environment.

9. Choose one of the following options.

   - If you are using the standard tape drive configuration listed in the **Check Your Tape Drive Configuration** procedure, earlier in this section, follow these instructions.

     a) Type **/cdrom/cdrom0/s3/backup_restore/backupDatabase** and then press **Enter.**

        Result: The system displays the following message:
        Please mount tape 1 on /dev/rmt/0h and then press Return to continue.

     b) Go to step 11.

   - If you are using a custom tape drive configuration, go to step 10.

10. If you are using a custom tape drive configuration, type **/cdrom/cdrom0/s3/backup_restore/backupDatabase -b [blocksize] -s [tapesize]** and then press **Enter**.

    Notes:

    - The [tapesize] refers to the tapesize that corresponds to your tape from the chart in the **Tape Considerations** section of Chapter 2.
    - The [blocksize] refers to the blocksize that corresponds to your tape from the chart in the **Tape Considerations** section of Chapter 2.

    Example:
    /cdrom/cdrom0/s3/backup_restore/backupDatabase -b 128 -s 13212058

    Result: The system displays the following message:
    Please mount tape 1 on /dev/rmt/0h and then press Return to continue.

11. Press **Enter**.

    Result: The system backs up your Informix database.

    Notes:

    - The system will prompt you to insert additional tapes if your backup requires more than one tape.
    - The message **Successfully completed the database backup** appears when the backup has completed successfully.
    - If the database backup was not successful, the system displays an error **message**. Call Cisco Services for assistance in resolving the error message.

12. Type **eject cdrom** and then press **Enter**.

13. Remove the CD and tape(s) and store them in a safe place.

Restore the Informix Database

Introduction

This section contains the following information:

- Default DNCS tape drive configuration information
- A procedure to determine the configuration of the tape drive in use on your system
- Procedures to restore the Informix database

Prevent the Loss of Data

When you restore the database, you restore it with data that was present in the database at the time of the backup. Unless you coordinate the restore procedures with your billing vendor, you run the risk of losing data that was transmitted to your system since the time of the backup. By adhering to the following guidelines, you can minimize the risk that you will lose data when you restore the database.

Follow these guidelines when restoring the database:

- Before restoring the database, contact your billing vendor and request that the billing vendor send no more transactions until the restoration is complete.
- If your system is still functional at the time of the restore, request that the billing vendor download from the DNCS the latest set of IPPV billing transactions before you start the restoration process. This way, you have the most current record of subscriber IPPV purchases.
- After completing the restoration of the database, contact the billing vendor and request that the billing vendor re-transmit all transactions since the date of the backup tape you used. For example, have the billing vendor re-transmit transactions relating to DHCT service levels, PPV event definitions, and package authorizations.
- Run the smMix utility between 12 and 24 hours after restoring the database in order to chart the expiration time of EMMs in the system.

  Notes:

  – This guideline is especially useful for sites that have restored a database from a tape that is more than 10 days old. When the database is restored, these sites are likely to be repopulated with EMMs that are due to expire in fewer than 20 days, resulting in an uneven distribution of EMMs. The smMix utility will help you decide whether these EMMS should be redistributed.

  – Refer to Chapter 10, **Chart EMM Expiration Times With the smMix Utility**, in *DBDS Utilities Installation Instructions and DNCS Utilities User's Guide*, part number 740020, for instructions on running the smMix utility.

Default Tape Drive Configuration

The script used by the DNCS to restore the Informix database uses the following default tape drive configuration:

- Tape size: 7549747 KB
- Block size: 32 KB
- Device name: /dev/rmt/0h

This tape drive configuration is the configuration in use on a majority of systems. Occasionally, however, the tape drive on a system may be configured with a different device name, such as /dev/rmt/1h.

Note: The 'h' that appears at the end of device name /dev/rmt/0h or /dev/rmt/1h indicates that the system is to use a high density format when writing to the tape.

The tape drive configuration that you use to restore the Informix database is the same configuration you used to back up the Informix database. If you are using a custom tape drive configuration, refer to step 5 in the **Checking Your Tape Drive Configuration** procedure (where you wrote it down) in the **Back Up the Informix Database** section, earlier in this chapter.

How Many Tapes Are in the Backup?

You may have been required to use more than one backup tape when you backed up the Informix database. Refer to one of the following procedures based on whether you used more than one backup tape.

- If you used only one tape to back up the Informix database, refer to the **Restoring the Informix Database Using One Backup Tape** procedure to restore the database.
- If you used more than one tape to back up the Informix database, refer to the **Restoring the Informix Database Using More Than One Backup Tape** procedure to restore the database.

Database Restore Script Options

The script that backs up the databases is called **restoreDatabase**. You can run the restoreDatabase script with the following options:

- *-l* — local-tape-drive. Specifies tape drive to use on local host (e.g. -- /dev/rmt/0h)
- -r — remote-tape-drive. Specifies tape drive on a remote host (e.g. – sparky: /dev/rmt/0h or 192.168.1.10: /dev/rmt/0h)
- *-check-database* — Checks the integrity of the databases (Does not fix if errors are found)
- *-verbose* — Verbose output

Restoring the Informix Database Using One Backup Tape

Follow these instructions to restore the Informix database using one backup tape.

Note: You need the tape from your most recent database backup in order to restore the Informix database.

Important: Be sure your tape is write-protected before you use it to restore the database.

1. If necessary, follow the procedures in Appendix A, **Stopping System Components**, to stop Spectrum, the Application Server, and the DNCS.
2. If necessary, open an xterm window on the DNCS.
3. Type **su -** and then press **Enter** to log in as root user.

   Note: Be sure to type the single dash after typing su.

   Result: The **password** prompt appears.
4. Type the root password and then press **Enter**.
5. Have you just restored the DNCS file system?
   - If **yes**, follow these instructions.
     a) Type **. /dvs/dncs/bin/dncsSetup** and then press **Enter**.

     Important: Be sure to type the dot prior to typing /dvs.

     Result: The system establishes the root user environment.

     b) Type **/export/home/informix/bin/formatDbSpace.sh** and then press **Enter**.

     Result: The system formats the database partitions.
   - If **no**, go to step 6.

6. Insert the CD labeled **DBDS Maintenance CD 2.0.x** into the CD drive of the DNCS.

7. Type **df -n** and then press **Enter**.

   Result: A list of the mounted filesystems appears.

   Note: The presence of **/cdrom** in the output confirms that the system correctly mounted the CD.

8. Insert your most recent copy of the DNCS database backup tape into the tape drive of the DNCS and wait for the green light on the tape drive to stop flashing.

9. Choose one of the following options.

   - If you are using the *standard* tape drive configuration listed in the **Check Your Tape Drive Configuration** procedure in the **Backup the Informix Database** section, earlier in this chapter, follow these instructions.
     a) Type **/cdrom/cdrom0/s3/backup_restore/restoreDatabase** and then press **Enter.**
     b) Go to step 11.
   - If you are using a *custom* tape drive configuration, go to step 10.

10. If you are using a custom tape drive configuration, type **/cdrom/cdrom0/s3/backup_restore/restoreDatabase -b [blocksize] -s [tapesize]** and then press **Enter**.

    Notes:

    - The [tapesize] refers to the tapesize that corresponds to your tape from the chart in the **Tape Considerations** section of Chapter 2.
    - The [blocksize] refers to the blocksize that corresponds to your tape from the chart in the **Tape Considerations** section of Chapter 2.

    Example:
    /cdrom/cdrom0/s3/backup_restore/restoreDatabase -b 128 -s 13212058

11. When the message **Is there more than 1 tape in this backup? [Y/N]** appears, type **n** and then press **Enter**.

    Result: The system displays a message about ensuring that the backup tape is in the drive.

12. Press **Enter**.

    Result: The system restores the database.

13. When the message **Successfully restored the database** appears, remove the tape and store it in a safe place.
14. Type **eject cdrom** and then press **Enter**.
15. Remove the CD and store it in a safe place.
16. Follow the procedures in Appendix B, **Restarting System Components**, to restart Spectrum, the DNCS, and the Application Server.

Restoring the Informix Database Using More Than One Backup Tape

Follow these instructions to restore the Informix database using more than one backup tape.

Note: You need the tapes from your most recent database backup in order to restore the Informix database.

Important: Be sure your tapes are write-protected before you use them to restore the database.

1. If necessary, follow the procedures in Appendix A, **Stopping the System Components**, to stop Spectrum, the Application Server, and the DNCS.
2. If necessary, open an xterm window on the DNCS.
3. Type **su -** and then press **Enter** to log in as root user.

   Note: Be sure to type the single dash after typing su.

   Result: The **password** prompt appears.
4. Type the root password and then press **Enter**.

5. Have you just restored the DNCS file system?
   - If **yes**, follow these instructions.
     a) Type **. /dvs/dncs/bin/dncsSetup** and then press **Enter**.

        Important: Be sure to type the dot prior to typing /dvs.

        Result: The system establishes the root user environment.

     b) Type **/export/home/informix/bin/formatDbSpace.sh** and then press **Enter**.

        Result: The system formats the database partitions.
   - If **no**, go to step 6.
6. Insert the CD labeled **DBDS Maintenance CD 2.0.x** into the CD drive of the DNCS.
7. Type **df -n** and then press **Enter**.

   Result: A list of the mounted filesystems appears.

   Note: The presence of **/cdrom** in the output confirms that the system correctly mounted the CD.
8. Choose one of the following options:
   - If you are using the *standard* tape drive configuration listed in the **Checking Your Tape Drive Configuration** procedure in the **Back Up the Informix Database** section, earlier in this chapter, follow these instructions.
     a) Type **/cdrom/cdrom0/s3/backup_restore/restoreDatabase** and then press **Enter.**
     b) Go to step 10.
   - If you are using a *custom* tape drive configuration, go to step 9.
9. If you are using a custom tape drive configuration, type **/cdrom/cdrom0/s3/backup_restore/restoreDatabase -b [blocksize] -s [tapesize]** and then press **Enter**.

   Notes:
   - The [tapesize] refers to the tapesize that corresponds to your tape from the chart in the **Tape Considerations** section of Chapter 2.
   - The [blocksize] refers to the blocksize that corresponds to your tape from the chart in the **Tape Considerations** section of Chapter 2.

   Example:
   /cdrom/cdrom0/s3/backup_restore/restoreDatabase -b 128 -s 13212058

10. When the message **Is there more than 1 tape in this backup? [Y/N]** appears, type **y** and then press **Enter**.

    Result: The system displays a message about ensuring that the last backup tape is in the tape drive**.**

    Note: You are instructed to load the last tape because a configuration file is appended to the final tape in the backup series during the backup procedure.

11. Insert the last tape from your most recent database backup and press **Enter**.

    Results:

    - The system examines the configuration file.
    - The system displays a message similar to the following:
      Please mount tape 1 on [device name] and press Return to continue.

12. Remove the tape that is currently in the tape drive.

13. Insert the first tape from your most recent database backup and press **Enter**.

    Results:

    - The system displays archive information from the tape.
    - The message **Continue restore? (y/n)** appears.

14. Type **y** and then press **Enter**.

    Result: The message **Do you want to back up the logs? (y/n)** appears.

15. Type **n** and then press **Enter**.

    Results:

    - The system begins restoring the database.
    - The **Please mount tape 2 on [device name] and press Return to continue** message appears after several minutes.

16. Remove the first tape and insert the second tape from your most recent database backup and then press **Enter**.

    Results:

    - The restoration of the database continues.
    - If there is another tape in the backup series, the system will prompt you to insert the next tape.

17. Repeat step 16 for as many backup tapes that are in the backup series.

18. When the message **Restore a level 1 archive? (y/n)** appears, type **n** and then press **Enter**.
19. When the message **Do you want to restore log tapes? (y/n)** appears, type **n** and then press **Enter**.
20. When the message **DNCS Informix partition restore completed and verified** appears, remove the final tape and store it in a safe place.
21. Type **eject cdrom** and then press **Enter**.
22. Remove the CD and store it in a safe place.
23. Follow the procedures in Appendix B, **Restarting System Components**, to restart the DNCS, the Application Server, and Spectrum.

Chapter 4
Backing Up and Restoring the DNCS and Application Server

Overview

Introduction

Use the procedures in this chapter to back up and restore the file system and key files of the DNCS and the Application Server.

System Shutdown No Longer Required for File System Backup

System operators no longer have to shut down their system in order to back up the DNCS or Application Server file system. The backup procedures reflect this change.

Important: Even though you are no longer required to shut down the system components, Cisco highly recommends that you schedule your file system backups for periods of lowest system activity.

In This Chapter

This chapter contains the following topics.

Topic	See Page
Back Up the DNCS or Application Server File System	4-2
Back Up the DNCS or Application Server Key Files	4-7
Restore the DNCS or Application Server File System	4-11
Restore the DNCS or Application Server Key Files	4-19

Back Up the DNCS or Application Server File System

Overview

Consider the following points about a backup of the DNCS or Application Server file system.

Recommended Frequency

Cisco recommends that system operators perform a complete system backup just prior to upgrading to new system software, as well as after the upgrade.

Backup Script Options

The script that backs up the file system is called **backupFileSystems**. You can run the backupFileSystems script with the following options:

- *-l* — local-tape-drive. Specifies tape drive to use on local host computer. (e.g. -- /dev/rmt/0h)
- -r — remote-tape-drive. Specifies tape drive on a remote host computer. (e.g. – sparky:/dev/rmt/0h or 192.168.1.10:/dev/rmt/0h)
- *-verbose* — Verbose output.

Failure of File System Backups and the ntpd Process

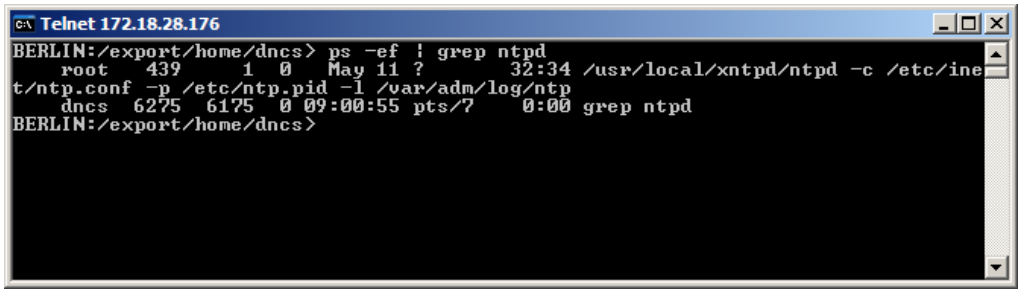
Occasionally, the file system backup of the DNCS or the Application Server may fail. If the backup fails, system operators should check that the ntpd process is running. The ntpd process needs to be running for the backup to succeed.

Note: The ntpd process is an operating system daemon that sets and maintains system time in synchronization with Internet standard time servers.

If the file system backup fails, system operators should follow this procedure to see if the ntpd process is running, and then to start it, if necessary.

1. From an xterm window on the DNCS or the Application Server (depending upon which file system backup failed), type **ps -ef | grep ntpd** and then press **Enter**.

   Result: The system reports whether the ntpd process is running.



2. Is the ntpd process running?
   - If **yes** (and the file system backup still failed), call Cisoc Services for assistance.
   - If **no**, follow these instructions to start the ntpd process.
     a) Type **su -** and then press **Enter** to log on to the xterm window as root user.
     b) Type the root password and then press **Enter**.
     c) Type **/etc/init.d/xntpd start** and then press **Enter**.
     d) Type **exit** and then press **Enter** to log out the root user.
3. Re-run the procedures to back up the file system.

Enterprise 450 and Sun Fire 880 Considerations

Before backing up the file system of an Enterprise 450 or Sun Fire 880 DNCS, Cisco recommends that system operators first check the dncs and root user e-mail accounts on the DNCS. The e-mail accounts will reveal whether any metadevice errors exist on the DNCS.

Preparing for the File System Backup

Follow this procedure to prepare for the DNCS or Application Server file system backup.

1. Are you backing up an Enterprise 450 or Sun Fire 880 DNCS?
   - If **yes**, check the dncs and root user e-mail accounts on the DNCS for the presence of metadevice errors.

     Note: Correct any metadevice errors before proceeding with the backup. Call Cisco Services if you need help in correcting metadevice errors.
   - If **no**, go to step 2.
2. If necessary, open an xterm window on the DNCS or Application Server, whichever server you are backing up.
3. Type **su -** and then press **Enter** to log in as root user.

   Note: Be sure to type the single dash after typing su.

   Result: The **password** prompt appears.
4. Type the root password and then press **Enter**.
5. Insert the CD labeled **DBDS Maintenance CD 2.0.x** into the CD drive of the DNCS or the Application Server, whichever server you are backing up.
6. Type **df -n** and then press **Enter**.

   Result: A list of the mounted filesystems appears.

   Note: The presence of **/cdrom** in the output confirms that the system correctly mounted the CD.
7. Label a blank tape with the following information:

   [DNCS or Application Server] File System Backup [Date]
   [Site Name]
   [Software Version]
   DBDS Maintenance CD 2.0.x

   Note: Customize the date, site name, and software version for the site you are backing up.

8. Choose one of the following options:
   - If you are backing up the file system to a tape in the DNCS or Application Server, go to **Backing Up the File System to the DNCS or Application Server**, next in this section.
   - If you are backing up the file system to a tape in a remote host computer, go to **Backing Up the File System to a Remote Host Computer**, later in this section.

Backing Up the File System to the DNCS or Application Server

Follow these instructions under the following circumstances:

- You are backing up the file system of the DNCS to a tape in the DNCS, itself
- You are backing up the file system of the Application Server to a tape in the Application Server, itself

If you are backing up the file system of the Application Server to a tape in the DNCS, use the procedure in **Backing Up the File System to a Remote Host Computer**, next in this section, instead.

Note: If you have correctly followed the directions in this chapter, you should be logged in to an xterm window as root user.

1. Insert the blank tape into the tape drive of the DNCS or Application Server, whichever server you are backing up, and wait for the green light to stop flashing.
2. To back up the file system, type **/cdrom/cdrom0/s3/backup_restore/backupFileSystems** and then press **Enter**.

   Result: The system backs up the DNCS or Application Server file system, ejects the tape, and displays a message when the backup is complete.
3. When the backup is complete, remove the tape and store it in a safe place.
4. Type **eject cdrom** and then press **Enter**.

Backing Up the File System to a Remote Host Computer

Follow these instructions to back up the DNCS or Application Server file system to a tape in another computer — commonly referred to as a *remote host* computer.

Example: Use this procedure, for instance, if you are backing up the Application Server file system to a tape in the DNCS.

Note: If you have correctly followed the directions in this chapter, you should be logged in to an xterm window as root user.

1. Insert the blank tape into the tape drive of the remote host computer.
2. At the DNCS or Application Server, whichever server you are backing up, type **rsh [hostname** or **IP address] pwd** and then press **Enter**.

   Notes:

   - Substitute the host name or the IP address of the remote host computer for [hostname or IP address].
   - The purpose of this command is to confirm that you can connect (remote shell) to the host computer without being prompted for a password.
3. Did the system prompt you for a password or deny you access after executing step 2?
   - If **yes**, call Cisco Services for assistance.
   - If **no**, go to step 4.
4. To back up the DNCS or Application Server file system, type **/cdrom/cdrom0/s3/backup_restore/backupFileSystems -r [hostname or IP address]**:**[tape device]** and then press **Enter**.

   Note: Type the entire command on one line.

   Examples:

   - **/cdrom/cdrom0/s3/backup_restore/backupFileSystems -r Wembly:/dev/rmt/0h**
   - **/cdrom/cdrom0/s3/backup_restore/backupFileSystems -r 192.168.44.71:/dev/rmt/0h**

   Result: The system backs up the file system, ejects the tape, and displays a message when the backup is complete.
5. When the backup is complete, remove the tape and store it in a safe place.
6. Type **eject cdrom** and then press **Enter**.
7. Remove the CD and store it in a safe place.

Back Up the DNCS or Application Server Key Files

Overview

Consider the following points about a backup of the DNCS or Application Server key files.

Recommended Frequency

The key files consist of those files required to boot the DNCS or Application Server. The script that backs up the file system also backs up the key files. For this reason, system operators need to back up the key files only when preparing for a system upgrade.

Backup Script Options

The script that backs up the DNCS and Application Server key files is called **backupKeyFiles.** You can run the backupKeyFiles script with the following options:

- *-I*—key_files_include. Specifies the file that lists all the files that need to be included in the backup
- *-E*—key_files_exclude. Specifies the file that lists all the files that need to be excluded from the backup
- *-l*— local-tape-drive. Specifies tape drive to use on local host computer (for example – /dev/rmt/0h)
- -r – remote-tape-drive. Specifies tape drive on a remote host computer (for example – sparky:/dev/rmt/0h or 192.168.1.10:/dev/rmt/0h)
- *-B*—Backup_Directory. Specifies the backup directory to which the key files should be saved (in tar format)

  Important: The system creates a file named KeyFiles.tar in the specified directory. If you wish to back up both the DNCS and the Application Server key files at the same time, be sure to specify different directories for both sets of key files, or one backup will overwrite the other.
- *-verbose*—Verbose output

Notes:

- The *–I* and *–E* options are independent of one another; any one of them may be used. If neither the *–I* or *–E* option is specified, then the default Keyfiles.include or Keyfiles.exclude files, which exist in the current directory, are used.
- If either the *–I* or *–E* option is included, the absolute path must be specified.
- The *–l* and *–r* options are mutually exclusive of one another; only one of them can be used.
- The *–B* option cannot be used if either the *–l* or *–r* option is used.

Preparing for the Key Files Backup

Follow this procedure to prepare to back up the DNCS or Application Server key files.

1. If necessary, open an xterm window on the DNCS or Application Server, depending on which server you are backing up.
2. Type **su -** and then press **Enter** to log in as root user.

   Note: Be sure to type the single dash after typing su.

   Result: The **password** prompt appears.
3. Type the root password and then press **Enter**.
4. Insert the CD labeled **DBDS Maintenance CD 2.0.x** into the CD drive of the DNCS or Application Server, depending on which server you are backing up.
5. Type **df -n** and then press **Enter**.

   Result: A list of the mounted filesystems appears.

   Note: The presence of **/cdrom** in the output confirms that the system correctly mounted the CD.
6. Label a blank tape with the following information:

   [DNCS or Application Server] Key Files Backup [Date]
   [Site Name]
   [Software Version]
   DBDS Maintenance CD 2.0.x

   Note: Customize the date, site name, and software version for the site you are backing up.
7. Choose one of the following options:
   - If you are backing up the key files to a tape in the DNCS or Application Server, go to **Backing Up the Key Files to the DNCS or Application Server**, next in this section.
   - If you are backing up the key files to a tape in a remote host computer, go to **Backing Up the Key Files to a Remote Host Computer**, later in this section.

Backing Up the Key Files to the DNCS or Application Server

Follow these instructions under the following circumstances:

- You are backing up the key files of the DNCS to a tape in the DNCS, itself
- You are backing up the key files of the Application Server to a tape in the Application Server, itself

If you are backing up the key files of the Application Server to a tape in the DNCS, use the procedure in **Backing Up the Key Files to a Remote Host Computer**, next in this section, instead.

Note: If you have correctly followed the directions in this chapter, you should be logged in to an xterm window as root user.

1. Insert the blank tape into the tape drive of the DNCS or Application Server, whichever server you are backing up, and wait for the green light to stop flashing.
2. Type **/cdrom/cdrom0/s3/backup_restore/backupKeyFiles** and then press **Enter**.

   Result: The system backs up the DNCS or Application Server key files and displays a message when the backup is complete.
3. When the backup is complete, eject the tape and store it in a safe place.
4. Type **eject cdrom** and then press **Enter**.
5. Remove the CD and store it in a safe place.

Backing Up the Key Files to a Remote Host Computer

Follow these instructions to back up the DNCS or Application Server key files to a tape in another computer — commonly referred to as a *remote host* computer.

Example: Use this procedure, for instance, if you are backing up the Application Server key files to a tape in the DNCS.

Note: If you have correctly followed the directions in this chapter, you should be logged in to an xterm window as root user.

1. Insert the blank tape into the tape drive of the remote host computer.
2. At the DNCS or Application Server, whichever server you are backing up, type **rsh [hostname** or **IP address] pwd** and then press **Enter**.

   Notes:

   - Substitute the host name or the IP address of the remote host computer for [hostname or IP address].
   - The purpose of this command is to confirm that you can connect (remote shell) to the host computer without being prompted for a password.
3. Did the system prompt you for a password or deny you access after executing step 2?
   - If **yes**, call Cisco Services for assistance.
   - If **no**, go to step 4.
4. To back up the DNCS or Application Server key files, type **/cdrom/cdrom0/s3/backup_restore/backupKeyFiles -r [hostname or IP address]:[tape device]** and then press **Enter**.

   Note: Type the entire command on one line.

   Examples:

   - **/cdrom/cdrom0/s3/**backup_**restore/backupKeyFiles -r Wembly:/dev/rmt/0h**
   - **/cdrom/cdrom0/s3/**backup_**restore/backupKeyFiles -r 192.168.44.71:/dev/rmt/0h**

   Result: The system backs up the DNCS or Application Server key files, ejects the tape, and displays a message when the backup is complete.
5. When the backup is complete, remove the tape and store it in a safe place.
6. Type **eject cdrom** and then press **Enter**.
7. Remove the CD and store it in a safe place.

Restore the DNCS or Application Server File System

Overview

Consider the following points about the restoration of the DNCS or Application Server file system.

Prerequisite

You need the tape from your most recent backup of the file system before restoring the file system.

Important: Be sure your tapes are write-protected before you use them to restore the system.

Restart of System Components

Upon completion of the restoration of the DNCS or Application Server file system, the system components are likely to restart automatically. This behavior is normal. If you intend to immediately restore the database, however, after restoring the file system, be certain that you stop the system components before restoring the database. The steps involved in restoring the database clearly direct you to stop the system components.

Restore Script Options

The script that restores the DNCS file system is called **restoreFileSystems**. You can run the restoreFileSystems script with the following options:

- *-l* — local-tape-drive. Specifies tape drive to use on local host computer (for example -- /dev/rmt/0h)
- -r — remote-tape-drive. Specifies tape drive on a remote host computer (for example – sparky:/dev/rmt/0h or 192.168.1.10: /dev/rmt/0h)
- *-verbose* — Verbose output

Note: The *–l* and *–r* options are mutually exclusive of one another; only one of them can be used.

Preparing to Restore the File System

Follow this procedure to prepare to restore the DNCS or Application Server file system.

Important: You need to know the IP address and the netmask of the DNCS or Application Server in order to complete this procedure.

1. Follow the procedures in Appendix A, **Stopping System Components**, to stop the system components.
2. Open an xterm window on the DNCS or Application Server, whichever server you are restoring.
3. Type **su -** and then press **Enter** to log in as root user.

   Note: Be sure to type the single dash after typing su.

   Result: The **password** prompt appears.
4. Type the root password and then press **Enter**.
5. Insert the CD labeled **DBDS Maintenance CD 2.0.x** into the CD drive of the DNCS or Application Server, whichever server you are restoring.
6. Are you restoring the DNCS file system?
   - If **yes**, follow these instructions.
     a) On the Application Server, type **shutdown -y -g0 -i0** and then press **Enter**.
     b) On the DNCS, type **shutdown -y -g0 -i0** and then press **Enter**.
   - If **no** (you are restoring the Application Server file system, only), type **shutdown -y -g0 -i0** and then press **Enter** on the Application Server.

   Result: The system halts all processes on the DNCS and/or Application Server and an **ok** prompt appears.
7. At the ok prompt on the server into which you have inserted the CD, type **boot cdrom - SAshell** and then press **Enter**.

   Result: The DNCS or Application Server boots into the OpenWindows environment.

   Notes:
   - When the system boots into the OpenWindows environment, it searches its non-volatile RAM for configuration information.
   - If the system is unable to locate its configuration information (a rare occurrence), it prompts you for the information it needs through the Solaris Installation menu.

8. In the process of booting, did the Solaris Installation menu appear?
   - If **yes**, follow these instructions.
     a) At the Solaris Installation menu, select **Continue**.
     b) At the Identify This System menu, select **Continue**.
     c) At the Hostname menu, type the hostname of the DNCS or Application Server and then select **Continue**.
     d) At the IP Address menu, type the IP address of the DNCS or Application Server and then select **Continue**.
     e) At the Subnets menu, select **yes** at the **System part of subnet** question and then select **Continue**.
     f) At the Netmask menu, type the netmask of the DNCS or Application Server and then select **Continue** (or just select **Continue** to accept the default value of 255.255.255.0).
     g) At the IPv6 menu, choose **No** and then select **Continue**.

        Result: The Confirm Information window opens that allows you to review all of the configuration information you have just submitted.
     h) Review the data on the Confirm Information window and correct anything that needs to be changed; then select **Continue**.
     i) At the Name Service window, select **None** and then select **Continue**.

        Result: The Confirm Information window reappears.
     j) Review the data on the Confirm Information window and correct anything that needs to be changed; then select **Continue**.

        Result: An xterm window opens.
     k) Go to step 9.
   - If **no** (the system successfully found the configuration information it needed), go to step 9.

9. Choose one of the following options:
   - If you are using the tape drive of the DNCS or Application Server to restore the file system, insert your most recent file system backup tape into the tape drive of the DNCS or Application Server, whichever server you are restoring.
   - If you are using the tape drive of a remotely located computer to restore the file system, insert your most recent file system backup tape into the tape drive of the remotely located computer.

10. Type **cd /tmp/cdrom/backup_restore** and then press **Enter**.

    Result: The /tmp/cdrom/backup_restore directory becomes the working directory.

11. Choose one of the following options:
    - If you are using the tape drive of the DNCS or Application Server to restore the file system, go to **Restoring the File System From the DNCS or Application Server**, next in this section.
    - If you are using the tape drive of a remotely located computer to restore the file system, go to **Restoring the File System From a Remote Host Computer**, later in this section.

Restoring the File System From the DNCS or Application Server

Follow these instructions under the following circumstances:

- You are restoring the file system of the DNCS from a tape in the DNCS, itself
- You are restoring the file system of the Application Server from a tape in the Application Server, itself

If you are restoring the file system of the Application Server from a tape in the DNCS, use the procedure in **Restoring the File System From a Remote Host Computer**, next in this section, instead.

Note: If you have correctly followed the directions in this chapter, you should be logged in to an xterm window as root user.

1. Type **./restoreFileSystems** and then press **Enter**.

   Result: The system restores the DNCS or Application Server file system and displays a message when the restoration is complete.

2. When the restoration is complete, remove the tape and store it in a safe place.

3. Type **/usr/sbin/shutdown -y -i0 -i6** and then press **Enter**.

   Result: The DNCS or Application Server reboots and the Common Desktop Environment (CDE) login window appears.

   Note: The Enterprise 450 and Sun Fire 880 DNCS will reboot a few times as part of the restoration process.

4. Log on to the CDE as **root** user.

5. Have you just restored the file system of a DNCS?

   - If **yes**, follow the **Restore the Informix Database** procedures in Chapter 3 to restore the Informix database. After restoring the Informix database, go to step 6.

     Important: The final few steps in restoring the Informix database require that you eject the DBDS Maintenance CD and restart the system components. Stop right before you eject the CD and restart the system components.

   - If **no** (you restore the file system of an Application Server), skip to step 9.

6. Have you just restored the file system of an Enterprise 450 DNCS or of a Sun Fire V880 DNCS?

   - If **yes**, go to step 7; you now need to enable disk mirroring.

     Note: The DBDS Maintenance CD should still be in the CD drive of the DNCS and you should still be logged in as root user to an xterm window.

   - If **no**, skip to step 9.

7. Type **/cdrom/cdrom0/mirrState -a** and then press **Enter**.

   Result: The system displays the following message:

   WARNING!
   Proceeding beyond this point will ATTACH all Controller 2 submirrors.
   Are you certain you want to proceed?

8. Type **y** and then press **Enter**.

   Result: The system enables the disk mirroring functions on the DNCS.

   Note: Depending upon your system configuration, it may take up to an hour for all of the data to become mirrored.

9. Type **eject cdrom** and then press **Enter**.

   Result: The system ejects the CD.

10. Click the right mouse button on the server you restored and select **Log Out**.

    Result: The root user logs off and the CDE window returns.

11. Log on to the CDE window as **dncs** user.

12. Does the Application Server display an **ok** prompt?
    - If **yes**, follow these instructions.
      a) Type **boot** at the **ok** prompt on the Application Server and then press **Enter**.
      b) Log on to the Application Server as **dncs** user.
    - If **no**, go to step 13.
13. Follow the procedures in Appendix B, **Restarting System Components**, to restart Spectrum, the DNCS, and the Application Server.

Restoring the File System From a Remote Host Computer

Follow these instructions to restore the DNCS or Application Server file system from a tape in another computer — commonly referred to as a *remote host* computer.

Example: Use this procedure, for instance, if you are restoring the Application Server file system from a tape in the DNCS.

Note: If you have correctly followed the directions in this chapter, you should be logged on to an xterm window as root user.

1. Type **/cdrom/cdrom0/s3/backup_restore/restoreFileSystems -r [hostname or IP address]:[tape device]** and then press **Enter**.

   Notes:

   - Substitute the hostname or IP address of the remotely located computer for [hostname or IP address].
   - Type the command on one line.

   Example:
   /cdrom/cdrom0/s3/backup_restore/restoreFileSystems -r 192.168.44.71:/dev/rmt/0h

   Result: The system restores the DNCS or Application Server file system and displays a message when the restoration is complete.

2. When the restoration is complete, eject the tape and store it in a safe place.

3. Type **/usr/sbin/shutdown -y -i0 -i6** and then press **Enter**.

   Result: The DNCS or Application Server reboots and the Common Desktop Environment (CDE) login window appears.

   Note: The Enterprise 450 and Sun Fire 880 DNCS will reboot a few times as part of the restoration process.

4. Log on to the CDE as **root** user.

5. Have you just restored the file system of a DNCS?

   - If **yes**, follow the **Restore the Informix Database** procedures in Chapter 3 to restore the Informix database.

     Note: After restoring the Informix database, go to step 6.

     Important: The final few steps in restoring the Informix database require that you eject the DBDS Maintenance CD and restart the system components. Stop right before you eject the CD and restart the system components.

   - If **no** (you restore the file system of an Application Server), skip to step 11.

6. Have you just restored the file system of an Enterprise 450 DNCS or of a Sun Fire V880 DNCS?
   - If **yes**, go to step 7; you now need to enable disk mirroring.

     Note: The DBDS Maintenance CD should still be in the CD drive of the DNCS and you should still be logged in as root user to an xterm window.
   - If **no**, skip to step 9.

7. Type **/cdrom/cdrom0/mirrState -a** and then press **Enter**.

   Result: The system displays the following message:

   WARNING!
   Proceeding beyond this point will ATTACH all Controller 2 submirrors.
   Are you certain you want to proceed?

8. Type **y** and then press **Enter**.

   Result: The system enables the disk mirroring functions on the DNCS.

   Note: Depending upon your system configuration, it may take up to an hour for all of the data to become mirrored.

9. Type **eject cdrom** and then press **Enter**.

   Result: The system ejects the CD.

10. Click the right mouse button on the server you restored and select **Log Out**.

    Result: The root user logs off and the CDE window returns.

11. Log on to the CDE as **dncs** user.

12. Does the Application Server display an **ok** prompt?
    - If **yes**, follow these instructions.
      a) Type **boot** at the **ok** prompt on the Application Server and then press **Enter**.
      b) Log on to the Application Server as **dncs** user.
    - If **no**, go to step 13.

13. Follow the procedures in Appendix B, **Restarting System Components**, to restart Spectrum, the DNCS, and the Application Server.

Restore the DNCS or Application Server Key Files

Overview

Consider the following points about the restoration of the DNCS or Application Server key files.

Prerequisite

You need the tape from your most recent backup of the key files before restoring the key files.

Important: Be sure your tapes are write-protected before you use them to restore the key files.

System Shutdown Required

In order to restore the DNCS or Application Server key files, system operators must shut down Spectrum, the DNCS, and the Application Server.

Restore Script Options

The script that restores the DNCS or Application Server key files is called **restoreKeyFiles**. You can run the restoreKeyFiles script with the following options:

- *-l* — local-tape-drive. Specifies tape drive to use on local host computer (e.g. -- /dev/rmt/0h)
- -r – remote-tape-drive. Specifies tape drive on a remote host computer (e.g. – sparky:/dev/rmt/0h or 192.168.1.10: /dev/rmt/0h)
- *-verbose* — Verbose output

Note: The *–l* and *–r* options are mutually exclusive of one another; only one of them can be used.

Preparing to Restore the Key Files

Follow this procedure to prepare to restore the DNCS or Application Server key files.

1. Follow the procedures in Appendix A**, Stopping System Components**, to stop Spectrum, the Application Server, and the DNCS.
2. If necessary, open an xterm window on the DNCS or the Application Server, depending upon which server you are restoring.
3. Type **su -** and then press **Enter** to log in as root user.

   Note: Be sure to type the single dash after typing su.

   Result: The **password** prompt appears.
4. Type the root password and then press **Enter**.
5. Insert the CD labeled **DBDS Maintenance CD 2.0.x** into the CD drive of the DNCS or Application Server, depending upon which server you are restoring.
6. Type **df -n** and then press **Enter**.

   Result: A list of the mounted filesystems appears.

   Note: The presence of **/cdrom** in the output confirms that the system correctly mounted the CD.
7. Choose one of the following options:
   - If you are going to restore the key files from a tape in the DNCS or Application Server, insert your most recent key files backup tape into the tape drive of the DNCS or Application Server, depending upon which server you are restoring, and wait for the green light to stop flashing.
   - If you are going to restore the key files from a tape in a remote host computer, insert your most recent key files backup tape into the tape drive of the remote host computer.
8. Choose one of the following options:
   - If you are using the tape drive of the DNCS or Application Server to restore the key files, go to **Restoring the Key Files From the DNCS or Application Server**, next in this section.
   - If you are using the tape drive of a remotely located computer to restore the key files, go to **Restoring the Key Files From a Remote Host Computer**, later in this section.

Restoring the Key Files From the DNCS or Application Server

Follow these instructions under the following circumstances:

- You are restoring the key files of the DNCS from a tape in the DNCS, itself
- You are restoring the key files of the Application Server from a tape in the Application Server, itself

If you are restoring the key files of the Application Server from a tape in the DNCS, use the procedure in **Restoring the Key Files From a Remote Host Computer**, next in this section, instead.

Note: If you have correctly followed the directions in this chapter, you should be logged in to an xterm window as root user.

1. Type **/cdrom/cdrom0/s3/backup_restore/restoreKeyFiles** and then press **Enter**.

   Result: The system restores the DNCS or Application Server key files and displays a message when the restoration is complete.

2. When the restoration is complete, eject the tape and store it in a safe place.

3. Type **eject cdrom** and then press **Enter**.

4. Remove the CD and store it in a safe place.

5. Are you restoring the key files of the DNCS?
   - If **yes**, follow these instructions.
     a) From an xterm window on the Application Server, type **su -** and then press **Enter**.
     b) Type the root password and then press **Enter**.
     c) On the Application Server, type **/usr/sbin/shutdown -y -g0 -i0** and then press **Enter**.

        Result: The Application Server shuts down and the **ok** prompt appears.

     d) On the DNCS, type **/usr/sbin/shutdown -y -g0 -i6** and then press **Enter**.

        Result: The DNCS reboots.

     e) Log on to the CDE of the DNCS as **dncs** user.
   - If **no** (you are restoring the key files of the Application Server, type **/usr/sbin/shutdown -y -g0 -i6** and then press **Enter**.

     Result: The Application Server reboots.

6. Is the Application Server still at the **ok** prompt?
   - If **yes**, follow these instructions.
     a) Type **boot** and then press **Enter**.
        Result: The Application Server reboots.
     b) Log on to the CDE of the Application Server as **dncs** user.
   - If **no**, go to step 7.
7. Follow the instructions in Appendix B, **Restarting System Components**, to restart Spectrum, the DNCS, and the Application Server.

Restoring the Key Files From a Remote Host Computer

Follow these instructions to restore the DNCS or Application Server key files from a tape in another computer — commonly referred to as a *remote host* computer.

Example: Use this procedure, for instance, if you are restoring the Application Server key files from a tape in the DNCS.

Note: If you have correctly followed the directions in this chapter, you should be logged in to an xterm window as root user.

1. Type **/cdrom/cdrom0/s3/backup_restore/restoreKeyFiles -r [hostname or IP address]:/dev/rmt/0h** and then press **Enter**.

   Note: Type the command on one line.

   Examples:

   - **/cdrom/cdrom0/s3/backup_restore/restoreKeyFiles -r Wembly:/dev/rmt/0h**
   - **/cdrom/cdrom0/s3/backup_restore/restoreKeyFiles -r 192.168.44.71:/dev/rmt/0h**

   Result: The system restores the DNCS or Application Server key files and displays a message when the restoration is complete.

2. When the restoration is complete, eject the tape and store it in a safe place.
3. Type **eject cdrom** and then press **Enter**.
4. Remove the CD and store it in a safe place.
5. Are you restoring the key files of the DNCS?
   - If **yes**, follow these instructions.
     a) From an xterm window on the Application Server, type **su -** and then press **Enter**.
     b) Type the root password and then press **Enter**.
     c) On the Application Server, type **/usr/sbin/shutdown -y -g0 -i0** and then press **Enter**.

        Result: The Application Server shuts down and the **ok** prompt appears.

     d) On the DNCS, type **/usr/sbin/shutdown -y -g0 -i6** and then press **Enter**.

        Result: The DNCS reboots.

     e) Log on to the CDE of the DNCS as **dncs** user.
   - If **no** (you are restoring the key files of the Application Server, type **/usr/sbin/shutdown -y -g0 -i6** and then press **Enter**.

     Result: The Application Server reboots.

6. Is the Application Server still at the **ok** prompt?
   - If **yes**, follow these instructions.
     a) Type **boot** and then press **Enter**.
        Result: The Application Server reboots.
     b) Log on to the CDE of the Application Server as **dncs** user.
   - If **no**, go to step 7.
7. Follow the instructions in Appendix B, **Restarting System Components**, to restart Spectrum, the DNCS, and the Application Server.

Chapter 5
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.

Appendix A
Stopping System Components

Overview

Introduction

Use the procedures in this appendix to stop the Spectrum Network Management Service (Spectrum), the Application Server, and the DNCS.

In This Appendix

This appendix contains the following topic.

Topic	See Page
Stop System Components	A-2

Stop System Components

Introduction

You may be required to stop the system components before backing up or restoring the system's file system or key files. Follow these instructions to stop Spectrum (if required), the Application Server, and the DNCS.

Important: Be sure to follow these instructions in the order they are presented.

Stopping Spectrum

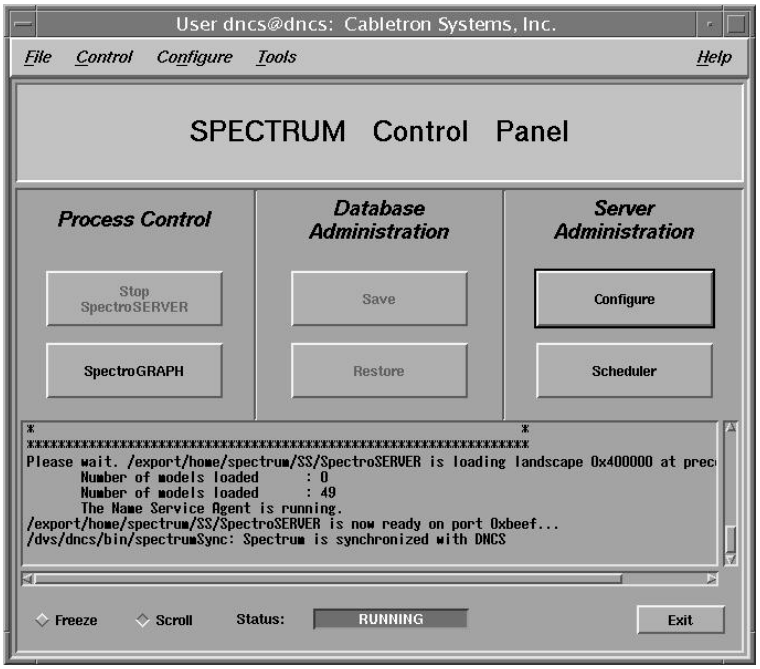
Complete these steps to stop Spectrum.

1. From the DNCS Administrative Console Status window, click **Control** in the NMS section of the window.

   Result: The Select Host to run on window appears.

2. From the **Select Host to run on** window, click **OK**.

   Result: The Spectrum Control Panel appears.



3. Click **Stop SpectroSERVER**.

   Result: A confirmation message appears.

4. Click **OK** at the confirmation message.

   Result: The **Status** message on the Spectrum Control Panel shows **Inactive.**

Continued on next page

5. Click **Exit** on the Spectrum Control Panel.

   Result: A confirmation message appears.

6. Click **OK** at the confirmation message.

   Result: The Spectrum Control Panel closes.

7. Go to **Stopping the Application Server**, next in this section.

Stopping the Application Server

Choose one of the following procedures based upon the resident application that runs on your system:

- For sites that support the Cisco resident application, follow the instructions in **Stopping the Application Server at SARA Sites**, next in this section.
- For sites that support the Pioneer resident application, follow the instructions in **Stopping the Application Server at Pioneer Sites**, later in this section.

Stopping the Application Server at SARA Sites

Complete these steps to stop the Application Server at sites that support the Cisco resident application.

1. Press the middle mouse button on the Application Server and select **App Serv Stop**.

2. From an xterm window on the Application Server, type **appControl** and then press **Enter**.

   Result: The Applications Control window appears.

3. Type **2** (for Startup/Shutdown Single Element Group), and then press **Enter**.

   Result: The system displays all Application Server processes.

   Note: The system updates the display periodically, or you can press **Enter** to force an update.

4. When the **Curr Stt** (Current State) field of the Applications Control window indicates that all of the Application Server processes have stopped, follow the on-screen instructions to close the Applications Control window.

5. Go to **Stopping the DNCS**, later in this section.

Continued on next page

Stopping the Application Server at Pioneer Sites

Complete these steps to stop the Application Server at sites that support the Pioneer resident application.

1. Press the middle mouse button on the Application Server and select **Passport Stop**.
2. From an xterm window on the Application Server, type **CheckServices** and then press **Enter**.

   Result: A list of drivers appears.

   Note: Each driver is associated with an Application Server process.
3. Wait until the word **No** appears next to each driver.
4. Go to **Stopping the DNCS**, next in this section.

Stopping the DNCS

Complete these steps to stop the DNCS.

1. At the DNCS, press the middle mouse button and then select **DNCS Stop**.
2. From an xterm window on the DNCS, type **dncsControl** and then press **Enter**.

   Result: The Dncs Control window appears.
3. Type **2** (for Startup/Shutdown Single Element Group), and then press **Enter**.

   Result: The system displays all DNCS processes.

   Note: The system updates the display periodically, or you can press **Enter** to force an update.
4. When the **Curr Stt** (Current State) field of the Dncs Control window indicates that all of the DNCS processes have stopped, follow the on-screen instructions to close the Dncs Control window.

What's Next?

Return to the instructions you were following when you were instructed to stop the system components.

Appendix B
Restarting System Components

Overview

Introduction

Use the procedures in this appendix to restart Spectrum, the DNCS, and the Application Server.

In This Appendix

This appendix contains the following topic.

Topic	See Page
Restart System Components	B-2

Restart System Components

Introduction

Follow these procedures to restart Spectrum, the DNCS, and the Application Server.

Restarting Spectrum

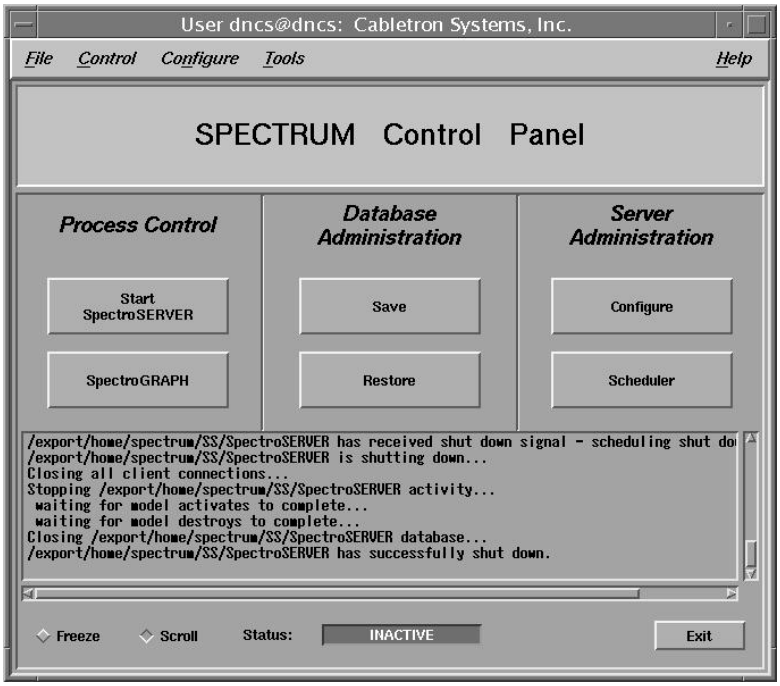
Follow these instructions to restart Spectrum.

1. From the DNCS Administrative Console Status window, click **NMS Control**.

   Result: The Select Host to run on window opens.

2. Select the Host Machine (usually DEFAULT), and then click **OK**.

   Result: The Spectrum Control Panel window opens.



3. On the Spectrum Control Panel window, click **Start SpectroSERVER**.

   Result: The Spectrum Network Management System starts.

4. On the Spectrum Control Panel window, click **Exit**.

   Result: A confirmation message appears.

5. Click **OK** on the confirmation message.

   Result: The Spectrum Control Panel window closes.

Continued on next page

Restarting the DNCS

Follow these instructions to restart the DNCS.

1. Click the middle mouse button on the DNCS and select **DNCS Start**.

   Results:

   - The DNCS processes start.
   - The DNCS Administrative Console Status window opens.

2. From the DNCS Administrative Console Status window, click **DNCS Monitor**.

   Results:

   - The DNCS Monitor window opens.
   - Green indicators replace red indicators on the DNCS Monitor window.

3. When all of the red indicators on the DNCS Monitor window have been replaced by green indicators, go to **Restarting the Application Server**, next in this appendix.

Continued on next page

Restarting the Application Server

When you rebooted the Application Server in the previous procedure, the Application Server processes probably restarted. Follow these instructions to check if the Application Server processes have started, and then to start them, if necessary.

Choose one of the following options:

- For sites on which the Cisco resident application runs on the Application Server, go to **Restarting the Application Server at SARA Sites**, next in this section.
- For sites on which the Pioneer resident application runs on the Application Server, go to **Restarting the Application Server at Pioneer Sites**, later in this section.

Restarting the Application Server at SARA sites

Follow these instructions to check if the Cisco application (SARA) has started on the Application Server, and then to start it, if necessary.

1. Open an xterm window on the Application Server.
2. Type **appControl** and then press **Enter**.

   Result: The Applications Control window opens.
3. Select option **2** on the Applications Control window.

   Result: The system displays a list of Application Server processes and their current status.
4. Does the word **running** appear next to the current state field (**Curr Stt**) of each process?
   - If **yes**, skip the rest of this procedure and go to **Restarting Spectrum**, later in this section.
   - If **no**, continue with step 5.
5. Press the middle mouse button, and then select **App Serv Start**.
6. When the Application Control window indicates that the current state (**Curr Stt**) of each process is **running**, go to step 7.

   Note: On some systems, the VOD Server process may remain at **Stopped**; this is normal.
7. Follow the onscreen instructions to close the Applications Control window.

Continued on next page

Restarting the Application Server at Pioneer Sites

Follow these instructions to check if the Pioneer application has started on the Application Server, and then to start it, if necessary.

1. Open an xterm window on the Application Server.
2. Type **CheckServices** and then press **Enter**.

   Result: A list of drivers appears.

   Note: Each driver is associated with an Application Server process.
3. Does the word **Yes** appear next to each driver?

   Note: The word **Yes** next to a driver indicates that the process has started.

   - If **yes**, skip the rest of this procedure and go to **Restarting Spectrum**, later in this section.
   - If **no**, continue with step 4.
4. Press the middle mouse button, and then select **Passport Start**.
5. When the word **Yes** appears next to each driver, go to step 6.
6. Follow the onscreen instructions to close the window containing the list of Pioneer drivers.

Appendix C
Setting Up an Automated Database Backup

Overview

Introduction

Cisco engineers have developed a UNIX cron script, called noinputDbBackup, which allows system operators to automate the nightly backup of their Informix database.

Note: A cron script is an automated process that operates at predefined time intervals. You may sometimes hear a cron script referred to as a cron job.

The noinputDbBackup script uses a modified version of the existing dncsDbBackup script to back up the Informix database with no user input. System messages pertaining to the execution of the noinputDbBackup script are written to a logfile in the /dvs/backups directory. The format of the logfile is noinputDbBackup.[DATE]_[TIME], where [DATE] and [TIME] refer to the date and the time the system executed the noinputDbBackup script.

To configure your system to execute the noinputDbBackup script, add an entry to the crontab on the DNCS. Use the instructions in this appendix to configure your system to execute the noinputDbBackup script.

In This Appendix

This appendix contains the following topic.

Topic	See Page
Configure the DNCS for an Automatic Database Backup	C-2

Configure the DNCS for an Automatic Database Backup

Verifying the Tape Drive Device Name

Before you configure your system for an automatic backup of the Informix database, confirm that the script that performs the backup uses the correct device name for the tape drive. Follow these instructions to confirm the correct device name.

1. Insert a blank tape into the tape drive of the DNCS.
2. Type **mt -f /dev/rmt/0 offline** and then press **Enter**.

   Important: The '0' in /dev/rmt/0 is zero.

   Result: If you have installed the tape drive correctly, the tape will eject.
3. Did the tape eject?
   - If **yes**, go to **Editing the crontab**, next in this appendix.

     Note: The device name of your tape drive is correct because the tape ejected.
   - If **no**, go to step 4.
4. Type the following UNIX routine.

   Important: Type the routine just as shown by pressing **Enter** at the end of each line.

   ```
   for drive in 0 1 2 3 4 5 6 7
   do
   mt -f /dev/rmt/$drive offline
   done
   ```

   Results:
   - The system tries to eject the tape using eight possible tape drive device names (/dev/rmt/0 through /dev/rmt/7).
   - The tape ejects when the UNIX routine reaches the correct device name.
   - The screen clearly shows which tape device name was used when the tape ejected.
5. In the space provided, note the device name that was used when the tape ejected. _____
6. Go to **Edit the noinputDbBackup.sh File**, next in this appendix.

Continued on next page

Edit the noinputDbBackup.sh File

Follow these instructions to edit the noinputDbBackup.sh file so that it includes the correct tape drive device name.

Note: The xterm window that you opened in the previous procedure, **Verifying the Tape Drive Device Name**, should still be open.

1. Type **vi /dvs/dncs/bin/noinputDbBackup.sh** and then press **Enter**.

   Result: The noinputDbBackup.sh opens for editing.

2. Scroll down through the file and locate the line that begins with **tapeDevice=/dev/rmt/0h**.

3. Edit the line so that it now references the device name you recorded in step 5 of the **Verifying the Tape Drive Device Name** procedure, earlier in this appendix.

   Example: tapeDevice=/dev/rmt/1h

4. Save the file and close the vi editor.

5. Go to **Editing the crontab**, next in this appendix.

Editing the crontab

Follow these instructions to configure your nightly backup of the Informix database on the DNCS.

1. From an xterm window on the DNCS, log in as **root** user.

2. Type **crontab -l > /tmp/root.crontab** and then press **Enter**.

   Important: The 'l' in crontab -l is a lowercase L.

   Result: The system redirects the contents of the crontab into root.crontab.

   Note: While you can edit the crontab directly, Cisco recommends that you first redirect the contents of the crontab to root.crontab so you can recover the original crontab if necessary.

3. Type **vi /tmp/root.crontab** and then press **Enter**.

   Result: The system opens root.crontab for editing using the UNIX vi editor.

Continued on next page

4. Add the following lines to the end of root.crontab:

   #cron to automatically back up the database
   0 2 * * * (. /dvs/dncs/bin/dncsSetup; /dvs/dncs/bin/noinputDbBackup.sh)

   Note: This command will back up the DNCS database at 2 AM everyday. To learn more about the various fields in the command you just entered, type **man crontab** and then press **Enter** at an xterm window on the DNCS.

5. Save the file and exit the vi editor.

6. Type **crontab /tmp/root.crontab** and then press **Enter**.

   Result: The system automatically backs up your DNCS database everyday.

Important Notes to the System Operator

The system will eject the tape after each backup. Remember to insert a blank tape into the tape drive of the DNCS each day. Cisco recommends that you store your daily tapes offsite to protect against loss or damage.

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

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

March 2012 Printed in USA

Part Number 4001155 Rev B