Maintenance Recommendations for the ISDS

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

Introduction

This guide helps you perform the maintenance tasks that keep your IPTV Services Delivery System (ISDS) in top condition. This guide includes normal maintenance tasks for the ISDS.

Purpose

After reading this publication, you should be able to perform maintenance tasks, such as checking disk partitions for space and backing up and restoring file systems, to identify possible issues before they become major problems.

Audience

This guide is written for system administrators and operators of the IPTV Service Delivery System (ISDS), as well as Cisco Services engineers and call-center personnel.

As many of the guidelines and checks in this document require the use of UNIX, readers should be proficient in UNIX.

Document Version

This is the third formal release of this document.

1

Daily ISDS Monitoring and Backup

Introduction

The ISDS is the key to all interactive system operations. The health of your ISDS is vital and should be monitored daily through the use of the tools and procedures outlined in this chapter.

In This Chapter

You've Got Mail From Solaris

Did you know the ISDS receives email every time Solaris detects a possible issue with the ISDS operating system? You can check the ISDS e-mail daily to ensure you address issues as needed.

What kinds of actions generate email? As one example, a task in cron will generate an email message if the task fails. Therefore, if cron runs an automated backup, and the backup fails, an email is generated. For some failures, the email message contains enough information to specify the exact problem.

Both root and the dncs role may receive mail from the system. Solaris will display a message indicating that a user has mail or new mail during the login process for that user:

```
Last login: Wed Aug  5 10:46:34 2009 from 64.100.119.30
Sun Microsystems Inc.   SunOS 5.10      Generic January 2005
You have new mail.
```

Checking Email

Complete the following steps to read email regarding your operating system.

1. Open an xterm window on the ISDS as root.
2. From the command line prompt, type **mail** and press **Enter**. If the ISDS has mail, the most recent email appears on the screen. If no mail exists, the message no mail appears.
3. Do you have mail?
   - If **yes**, read the message and press **Enter** when you are ready to go to the next message.
   - If **no**, type **q** and press **Enter** to exit email.

   Tips:
   - You can type ? and press Enter to see a menu of other commands and an explanation of those commands.

     Note: If the system display s a message **mail: Cannot open savefile** when you exit the mail program, complete the steps in ***Resolve Failure to Delete Mail Issue*** (on page 3).
   - Want to delete an email message you are viewing? You can delete email by typing d and pressing Enter.
4. When you have finished reading the ISDS email, type **q** and press **Enter** to exit email.
5. Repeat this procedure using the dncs role.

Resolve Failure to Delete Mail Issue

Complete the following steps if the system returns "mail: Cannot open savefile" when exiting the mail utility after deleting mail messages.

1. Open an xterm window on the ISDS as root.
2. Type **mkdir /var/mail/:saved** and press **Enter**.
3. Type **chmod 775 /var/mail/:saved** and press **Enter** to set the appropriate permissions.
4. Type **ls -ld /var/mail/:saved** to verify the permissions were set correctly for the new directory.

   Example:

   ```
   drwxrwxr-x   2 root     root         /var/mail/:saved
   ```

5. Go back to ***Checking Email*** (on page 2) to check and delete e-mail as necessary.

Reviewing the Administrator Messages File

Become familiar with the messages in the /var/adm/messages file to develop a sense for normal traffic. Checking this file regularly will help you distinguish normal traffic from possible issues. You can also filter this file for any messages containing a text error or warning. For example, you can use the grep command to filter on the words error and warning.

Check this directory anytime your system locks up randomly or experiences a hardware failure.

Complete these steps to review the administrator messages file.

1. From an xterm window, type **vi /var/adm/messages** and press **Enter**. All messages in the /var/adm/messages file are listed.
2. Type **egrep -i 'error|warning' /var/adm/messages** and press **Enter**. Any messages containing the text error or warning are listed.

   Important: Be sure to include a space after egrep, after -i, and after 'error|warning' in the above command.
3. Review error messages and warnings. If you find an error or warning you cannot resolve, contact Cisco Services.

Reviewing the Log File

Review the ISDS log files each morning to find out about any late-breaking issues that have occurred since the previous day. Check the file during the day if you suspect any issues.

Reviewing the Log File

Complete these steps to review the ISDS log file (dncsLog).

1. From an xterm window, type **cd /var/log** and press **Enter**.
2. The ISDS log is a very large file; a full day could reach 10 MB or more. To reduce the amount of data to review, type **tail -f dncsLog** and press **Enter**.

   Note: The tail command alone prints the last 20 lines of the log file. Adding the -f parameter to the tail command alerts you to any immediate issues because it continues to display new messages as they are added to the log.
3. Look for anything that contains an error message for several minutes.
4. Type **egrep -i 'error|fail' /var/log/dncsLog** and press **Enter**. Any messages containing the text error or fail are listed.

   Important: Be sure to include a space after egrep, after -i, and after 'error|fail' in the above command.
5. If you want, you can view the entire log file by typing **view dncsLog** and pressing **Enter**.

   Note: Viewing the entire log file is optional.
6. Look for the types of messages detailed in the next section. If you are looking for a specific message, use filtering commands to find the information you want.

   Example: You can find QPSK errors by entering **grep QPSK dncsLog | more**.

Looking for Messages in the ISDS Log File

When reviewing the ISDS log file, look for the following types of messages:

- Communication errors of any kind (comm lost, connection lost, etc.)
- Set-top UNConfig fail. Be especially aware if you have never seen this error before, or if it suddenly appears in large numbers when it was previously present in small numbers
- Any instances of processes stopping and restarting (usually creating a core file)
- Any changes from the normal appearance of the log
- Any errors relating to dsm or drm

Messages You Can Ignore

Many of the messages in the dncsLog are simply statuses and do not indicate any problem. When reviewing the ISDS log file, you can ignore the following types of messages:

- bfsRemote copy failed messages, if they occur only a few times after the bfsServer and bfsRemote processes, or all the processes, have been restarted
- bfsServer cancelled module messages

Managing Your Space

We recommend that you check the current disk space on your ISDS as a part of your daily system checks.

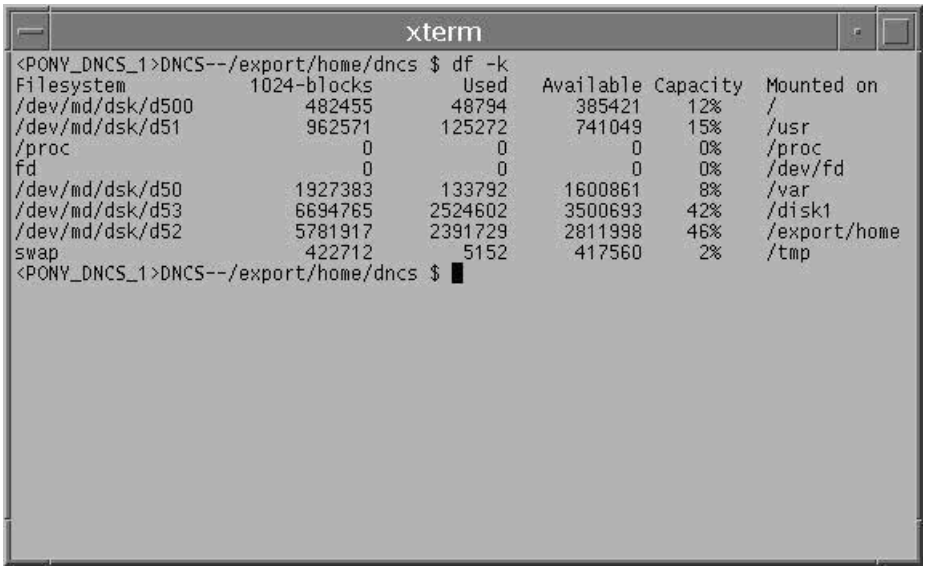
Note: You can perform the following procedure to check disk space, or you can view disk space statistics in the Doctor Report.

Checking Current Disk Space

To check the disk space on the ISDS and Application Server, complete these steps.

1 From an xterm window, type **df -k** and press **Enter** on the workstation for which you want to check the disk space. A list of filesystems and disk space appears in the xterm window.

Note: Be sure to type a space between df and -k in the above command.



2 Review the percent of capacity used for each partition. If you are nearing maximum capacity for a partition, move or delete files that are no longer needed.

Interpreting Disk Space Statistics

Refer to the following guidelines when interpreting disk space statistics:

- If / filesystem (root) is over 50%, find out why and monitor to see if it is increasing. If / is full, the system will fail.
- If /tmp is over 50% and increasing, start looking for memory leaks. Remember this directory is used for memory swap space, which is vital for proper operation of the system. Do not use /tmp for temporary file storage. If /tmp has been used for temporary file storage, clean out unnecessary temporary files that have been placed here. Any file in this directory is deleted if the system is rebooted.

- If /var is over 80% and increasing, you may want to save old log files at your discretion. There are three log files: dncsLog (today), dncsLog.0 (yesterday), and dncsLog.1 (day before yesterday). If these logs are very large, you can save them (except for today's log file) on an external device or a different disk partition that has plenty of available space. After saving off these files, delete them from the /var disk partition. In the rare cases that today's log file is filling the entire space, empty the contents of the current log. Either of these actions requires root access. See ***Removing the Contents of the Current Log File*** (on page 8) for specific instructions. If /var is over 80% and growing, you should also check to ensure tracing levels are not set unnecessarily high.
- If /disk1 is over 70%, monitor this disk closely. If over 80%, start looking for problems, typically process logs, but sometimes corefiles.
- If /export/home is over 70% and increasing, monitor this disk closely.

Removing the Contents of the Current Log File

To remove the contents of the log, complete these steps.

1. From an xterm window on the ISDS, log in as **root**.
2. Type **cd /dvs/dncs/etc** and press **Enter**.
3. Type **./newdncslog** and press **Enter**. The current content of the log file is compressed and moved to the dvs/dncs/tmp directory. The log file will begin accumulating new content.

Pinpointing Files to Delete

To find offending files when running out of space, complete these steps.

1. From an xterm window on the ISDS, go to the highest level of the file system that is running out of space, for example, /, /export/home, /dvs, /disk1.
2. Type **du -k | sort -rn |more** and press **Enter**. The output displays the largest directories and files in the file system beginning with the largest.

Checking Your Memory

You can use a UNIX utility called "Top" to monitor the percentage of CPU (Central Processing Unit) resources used by specific system processes. Run the Top utility periodically to ensure your memory usage is in a normal range for your system.

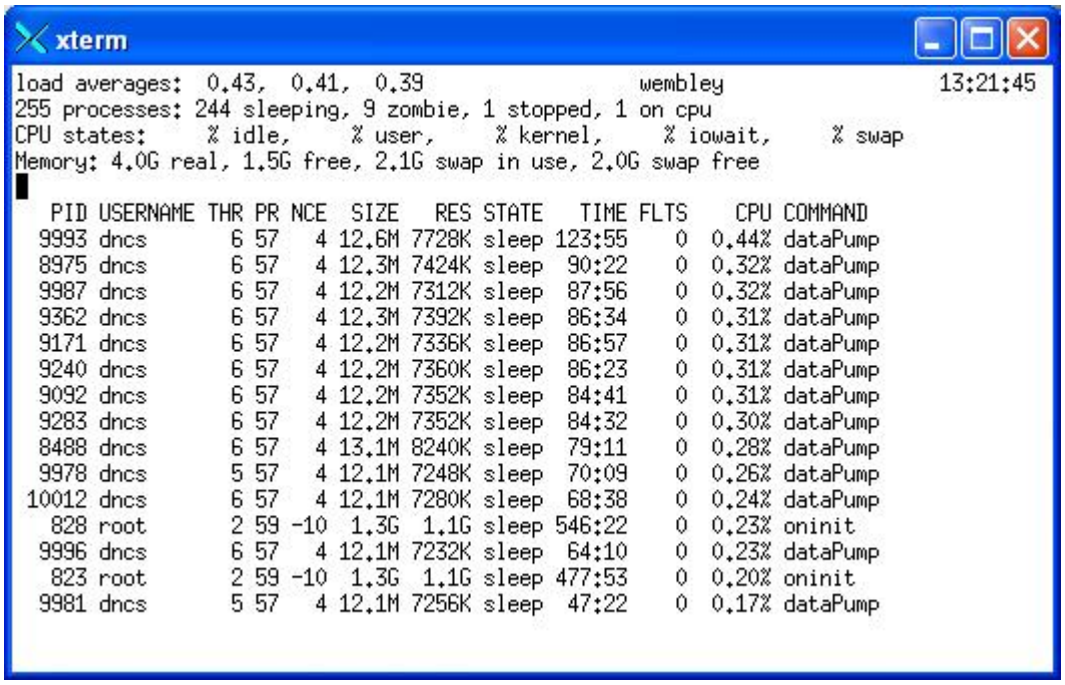
Note: You can perform the following procedure to check memory use, or you can view memory statistics in the Doctor Report.

Checking Memory with the Top Utility

Complete these steps to run the Top utility.

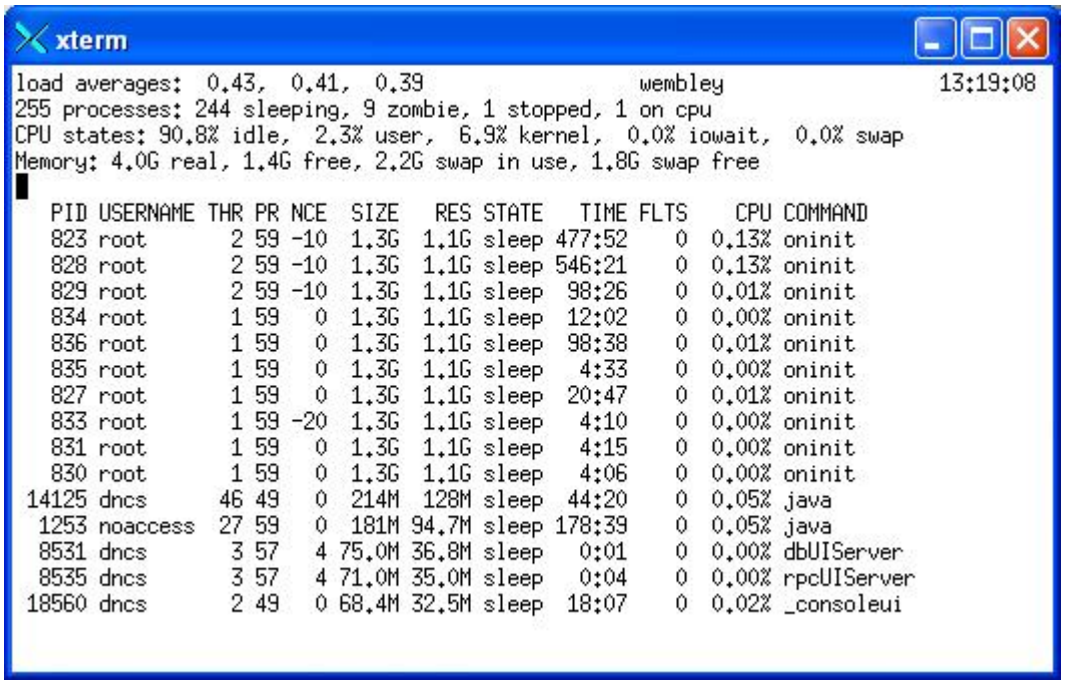
1. Open an xterm window on the ISDS.
2. Type **top** and press **Enter**. Output from the Top utility appears in the xterm window.

   Note: The xterm window containing the output from the Top utility updates automatically every few seconds.
3. Type **c** to highlight upper threshold issues in color.



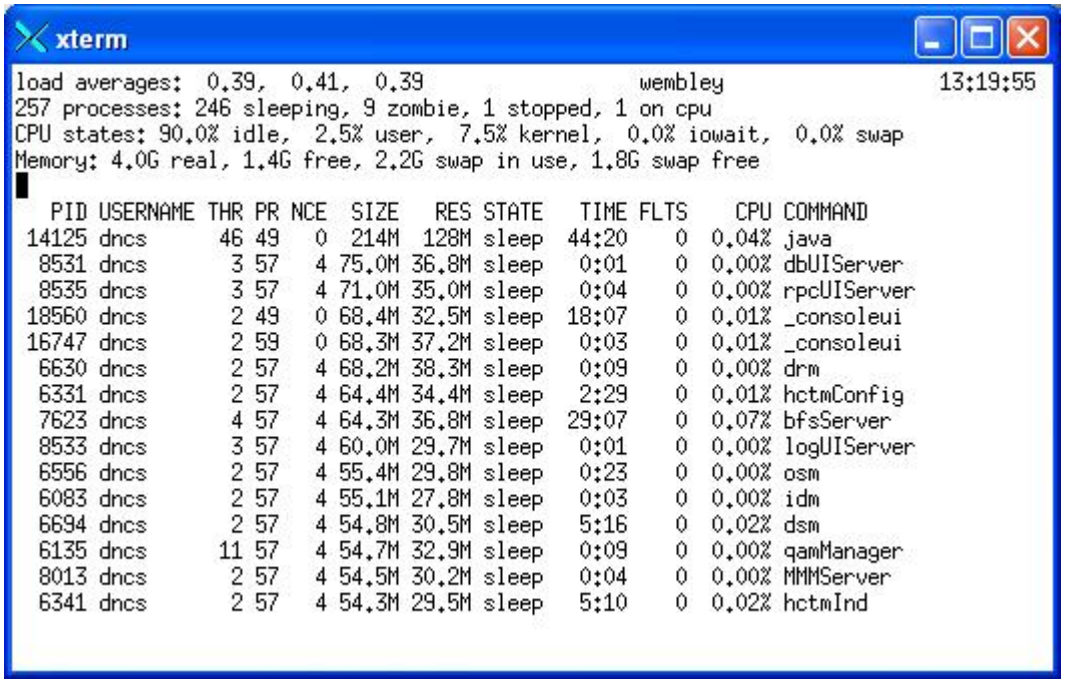
4. Type **o** (the letter "o") to get the Order to Sort prompt. Then press **Enter.**

5 Type **size** and press **Enter.** The information is sorted by the total amount of memory allocated by each process.

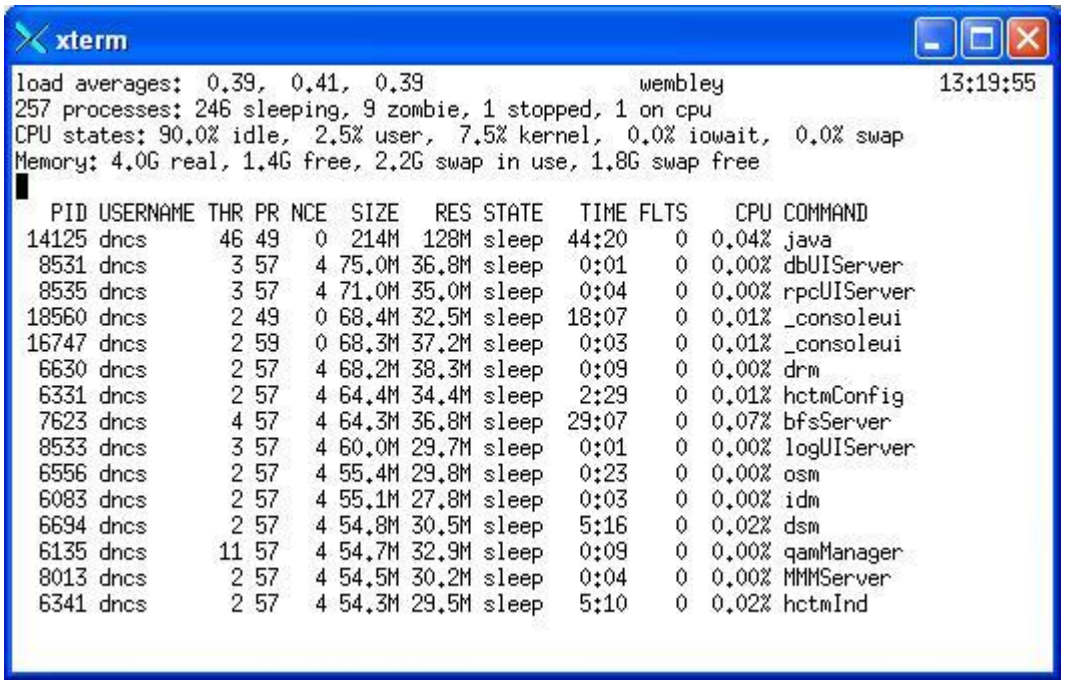


6 Type **u** and press **Enter.**

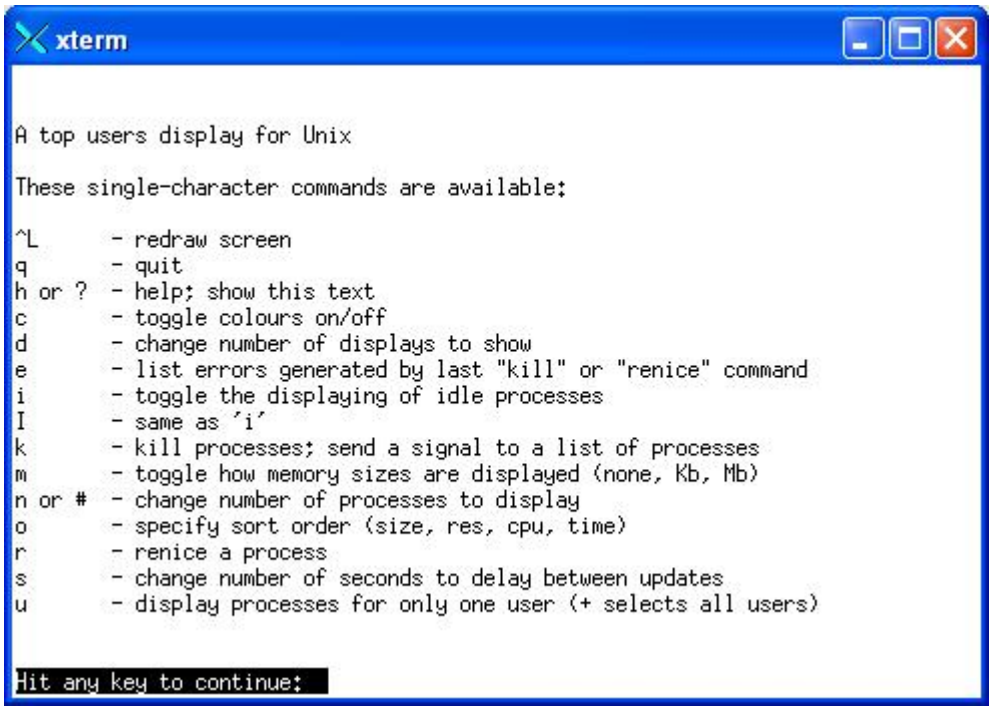
7 At the username to show prompt, type **dncs** and press **Enter.** The Top utility shows all processes that are owned by the dncs user.



8 If desired, you can view information by another sort order, such as the percentage of the CPU that each process is currently consuming.



9 For additional information on sort options and other commands, type **?** to view the latest help message. Type **q** to exit help.



10 When you have finished viewing information in Top, type **Ctrl+C** and press **Enter** to exit the utility.

11 If you need help reading output from Top, refer to the output descriptions compiled available on the Top utility website (http://www.unixtop.org/).

Reading Output from Top

If you need help reading output from Top, refer to the output descriptions compiled available on the Top utility website (http://www.unixtop.org/).

2

Analyze System Configuration with the Doctor Report

Introduction

The Doctor Report is one of the most important tools that system operators and support engineers can use to evaluate the configuration and operation of a network. Output from the Doctor Report appears on the screen of the ISDS and is written to an output file for later analysis.

The Doctor Report was developed to generate a snapshot of system configuration. The following list contains some of the system configuration information reported by the Doctor Report:

- Installed software versions
- ISDS and Application Server disk partition utilization
- Status of ISDS and Application Server processes
- Summary of supported DHCT types
- Summary of sources, source definitions, segments, and sessions
- Summary of PPV services and events
- Data carousel/pump status and rates
- Configuration data for remote sites
- Common configuration errors that may lead to problems later

Important: We strongly recommend that system operators run the Doctor Report at least once a day.

This chapter provides the following information about the Doctor Report:

- Running the Doctor Report
- Understanding the data produced by the Doctor Report

In This Chapter

Run the Doctor Report

Use the following procedure to run the Doctor Report on the ISDS.

1. If necessary, open an xterm window on the ISDS.
2. Type **cd /dvs/dncs/Utilities/doctor** and press **Enter**. The /dvs/dncs/Utilities/doctor directory becomes the working directory.
3. Type **doctor** and press **Enter**. The system generates a list of parameters that you can use to run the Doctor Report.

   Note: Each parameter causes the Doctor Report to generate output with specific configuration information.

```
scooby:/dvs/dncs/Utilities/doctor$ doctor

= Doctor sofware version 6.2.0.2 =
= Doctor package version  =
  doctor -agestpbinqhcrx [ vd ] or
  doctor [-c<number>]

        a - (almost) All options (except q and x)
        g - General Info: DNCS info, installed software info, DNCS and
            App Server disk utilization, DNCS and App Server swap space,
            database utilization, database extents, load average, DNCS
            and App Server debug flags, tracing levels, DNCS and App
            Server processes, DNCS and App Server corefiles, DNS, check
            force tune for valid service, dncs license check, large log file che
ck
            DNCS install options
        e - Element Info: DHCT state summary, DHCT type summary, active
            elements, mod slot tolerance, source, source definitions,
            segments, sessions, subscription packages, EMMs expiring soon.
        s - SI Info: SI_INSERT_RATE, system time message, distinguished
            SI QAM, SI out of band interval.
        t - Time Info: DNCS and App Server time sync, timezone, DST.
        p - PPV Info: PPV services and events, PPV and SAM service
            discrepancies, event use services, PPV files, phoneactivetime,
            EUT, GBAMs.
        b - BFS Info: BFS carousels, BFS sessions, BFS source definitions.
        i - IPG Info: IPG collector, IPG data files.
        n - Ping Elements: QPSK Ethernet, QPSK RF, QAM, NETCRYPT, BIG, TED.
        q - Check for quarantined qams and ping elements.
            This option is NOT included in all (-a).
        x - Check one-one correspondence of DHCTs and serial numbers.
            This option is NOT included in all (-a).
        v - Verbose mode: Detailed output, even if OK.
        d - Suppress screen output. Write to output file only.
        h - Generate this help text.
        c - Clean up (delete) all but the last <number> doctor reports.
            Use this switch independently of all others. Report NOT GENERATED.


        r - and one of the following options:
            hubqamList      - list what hub are associated to which QAMs
            smdgInfo        - list SMDG (StatMUX Dejitter Group) and respective
GQAM
            sdbsgInfo       - list SDB Service Group Mini Carousel Info
            genericQamInfo  - display generic QAMs and IPs
            dualGbeGqamInfo - display generic QAMs and IPs
            sdbInfo         - display SDB server info and status
            pcgInfo         - display PCGs info and status


One or more of the a, g, e, s, t, p, b, i, n, c, x or q options is required.
d and v are optional but should be used with a required option.
Option order is irrelevant.

        Note the q option must be explicitly chosen.  It can be time consuming.
        The q option automatically sets the v (verbose) option and pings and che
cks rpc bind for qams.
scooby:/dvs/dncs/Utilities/doctor$
```

4. To generate a complete Doctor Report, type **doctor -av** and press **Enter**.

   Results:

   - The system generates the Doctor Report listing all system configuration information and directs the output of the report to the screen.
   - The system also saves the output of the Doctor Report to a file in the current directory on the ISDS.

Example: The system saves the report with a name similar to **report.061026_0921.doc**.

Notes:

- Depending upon the size of your system, it may take a few minutes for the report to generate.
- The final line of the report generated to the screen lists the file to which the output was saved.
- The report is a plain text file. You can view the report in a text editor of your choice.

Test the Connection to the ISDS (-q Option of the Doctor Report)

The Doctor Report includes the *–q* option. Through the *–q* option, system operators can ping the modulators and test the connection between the modulators and the ISDS. Furthermore, the *–q* option generates a report that lists all the modulators, specifies whether the modulators are in a quarantined condition, and notes the date and time stamp of the quarantine, if applicable.

Understand the Data in the Doctor Report Fields

The information in this section provides an explanation of the data produced by generating the Doctor Report. Some of the data is only for informational purposes. Other data is preceded by the words **OK, Error**, or **Warning**.

Data in the report preceded by the word OK indicates that the data meets our recommendations regarding the field to which the data applies. Data in the report preceded by the word Error may indicate that some system process or function is not operating as it should. Where appropriate, this section includes troubleshooting tips so that system operators can investigate and correct a situation producing an error in a data field. A warning indicates that a potentially serious condition, such as a disk partition nearing capacity, or that certain data does not meet our recommendations, has been detected.

Important: Anytime an unexpected or new error appears in the Doctor Report output or if defined thresholds are about to be reached, contact Cisco Services for assistance.

System Name

The System Name field appears at the top of the Doctor Report, and displays the operational mode of the system. This field can be customized by the system operator to display the name of the system whose data is displayed in the report.

Note: If the System Name field does not reflect the name of your system, follow the instructions in **Customize the Doctor Report** in *DBDS Utilities Version 6.3 User Guide for the IBDS* (part number 4028578).

All SAI Installed Package Information

The data in the All SAI Installed Package Information field contains the following information about the software packages installed on your system:

- The name of the package
- The version number of the package
- The date the package was installed
- The platform on which the package was installed

ISDS Info

Data fields included under ISDS Info contain information that pertains to the hardware configuration of your ISDS.

ISDS Uptime

The ISDS Uptime field shows how long the ISDS processes have been running without interruption.

Note: To determine how long the ISDS processes have been running without interruption, the Doctor Report examines the **bootpd** process and determines how long the bootpd process has been running without interruption. The bootpd process is usually only restarted when the ISDS processes are reset.

Solaris Uptime

The Solaris Uptime field shows how long the Solaris operating system processes have been running without interruption.

Swap Space

The Swap Space field lists the configured swap partitions in the ISDS and how large they are.

System Configuration

The System Configuration field contains configuration information that pertains to the central processing unit (CPU) of the ISDS.

Memory Size

The Memory Size field displays how much physical memory is installed in the ISDS.

Virtual CPUs

The Virtual CPU field is seen only on the UltraSPARC T2 sun4v architecture. The two CPUs have a total of 16 cores (2x8). However, they configure themselves as 128 virtual processors. Each of these processors acts like a real processor, which allows the sun4v architecture to support multi-threaded applications.

This section lists all 128 virtual processors (0-127) and reports if they are online.

Physical Memory Configuration

This field reports on the amount of installed memory in the server, as well as how that memory is arranged (for example, in banks of 4 GB). The banks of memory may change due to changes in the dual in-line memory module (DIMM) design, but the overall memory will remain constant.

IO Devices

This field lists all of I/O devices attached to the server.

Disk Info

The Disk Info field displays configuration information for the server from a partition point of reference (rather than a metadevice point of reference).

Additionally, the Disk Info field reports on the configuration of the server's mirrors.

Checking the Status of the Meta Devices of the System

The Checking the Status of the Meta Devices of the System field reports on the status of the system's mirrored disks and reports any disks that have failed.

ISDS Service Delivery Server

The ISDS Service Delivery Server field contains the host names or IP addresses of various components of the ISDS.

ISDS Configuration Summary

The Hub Summary portion of the ISDS Configuration Summary field lists the ID, name, and multicast IP address if the configured hubs on the server.

The Cluster Summary portion of the ISDS Configuration Summary field lists configuration data for the system's clusters.

The Periodic UN-Config interval field shows the interval for UN-Config messages.

ISDS Disk Partition Utilization

The data in the ISDS Disk Partition Utilization field lists all the disk partitions on the ISDS and displays the "in-use" percentage of each partition.

Important: Our engineers recommend that no partition exceed 85 percent utilization.

Note: To decrease partition utilization, you can delete files that are no longer needed and core files that do not require analysis.

ISDS Swap Space

The data in the ISDS Swap Space field lists the amount of available swap space on the ISDS.

Important: Our engineers recommend that the ISDS swap space be greater than 1 GB.

Note: Completing the following tasks may increase your swap space:

- Close windows that do not need to be open.

- Stop and restart the ISDS.
- Run the **/usr/local/bin/top** utility and look for processes that use more than 50 MB of swap space. Use the dncsControl utility to stop and restart those processes.
- Look for large files in the /tmp directory. You can delete them or move them to another file system.

Basic System Performance Stats

There are 5 sets of performance statistics reported under the Basic System Performance Stats header. An explanation of each set follows.

CPU Performance

The CPU Performance field uses the prstat utility to iteratively examine all active processes on the system. As used in the Doctor Report (prstat -c 5 5), the prstat utility sorts output according to CPU usage, takes CPU measurements in 5-second intervals, and issues five separate reports.

Memory Usage

The Memory Usage field uses the prstat utility to iteratively examine all active processes on the system and report upon memory usage of the processes. As used in the Doctor Report (prstat -s size -c 5 5), the utility sorts output according to the size of the process image, takes memory measurements in 5-second intervals, and issues five separate reports.

Per-Processor Stats

The Per-Processor Stats field uses the mpstat utility to report processor statistics in tabular form. Each row in the tabular output represents the activity of one processor. The first table summarizes all processor activity since the last reboot. Subsequent tabular output summarizes activity for the preceding, specified interval. All values in the output are rates listed as events/second, unless specifically noted.

The mpstat utility, as used in the Doctor Report (mpstat 5 5), collects processor statistics in 5-second intervals and produces five reports.

Virtual Memory Stats

The Virtual Memory Stats field uses the vmstat utility to report statistics about kernel threads in the run and wait queue, memory, paging, disks, interrupts, system calls, context switches, and CPU activity.

As used in the Doctor Report (vmstat 5 5), the vmstat utility collects virtual memory statistics every 5 seconds and issues five separate reports.

Disk Stats

The Disk Stats field uses the iostat utility to iteratively examine terminal, disk, and tape input/output activity, as well as CPU utilization. The first line of output pertains to the time since the last reboot. Subsequent lines pertain to the specified prior interval, only.

For the Doctor Report (iostat -xPnMz 5 5), the utility produces extended statistics and displays names in descriptive per-partition format (rather than per-device format). Data is displayed in MB/second terms. The utility collects statistics every 5 seconds and issues five separate reports.

ISDS Database Check

The data in the ISDS Database Check field summarizes the usage of tempspace and dataspace in the ISDS database.

Important: This data should be interpreted only by those individuals knowledgeable in database management.

Database Spaces and Chunks

The Database Spaces and Chunks field reports on the contents and structure of the database shared memory by running the Informix *onstat -d* command.

Important: This data should be interpreted only by those individuals knowledgeable in database management.

Database Extents for dncsdb

The data in the Database Extents for dncsdb field lists the number of extents associated with specific tables in the ISDS database.

Note: The number of database extents refers to the number of times a specific table is fragmented across the hard drive.

Database Extents for appdb

The data in the Database Extents for appdb field lists the number of extents associated with specific tables in the Application Server database.

Database Backup Check

This field reports on the presence of a cron job to automatically back up the ISDS databases. If a cron job is present, this field reports whether the previous database backup was successful or if it failed.

Notes:

- A cron job is a program that runs automatically, without user intervention.
- The program that automatically backs up the database is a shell script called noinputDbBackup.sh. Your most recent system upgrade installation instructions may contain an appendix that describes how to configure your system for the automated database backup. The title of the appendix is **Setting Up an Automated Database Backup**.

Check for clearDbSessions Activity

The Doctor Report checks to ensure that the clearDbSessions entry in the crontab file of the ISDS is active, and has not been converted into a comment.

ISDS Load Average

The data in the ISDS Load Average field shows the average number of ISDS processes simultaneously waiting for CPU time on the previous day.

Important: Our engineers recommend that your ISDS load average remain under 2.0.

Note: The Doctor Report can determine the ISDS Load Average only if the Solaris **sar** utility is running. Refer to the UNIX man pages if you need to enable the sar utility.

Appserv Tracing Levels

The Application Server on the ISDS allows you to configure the level of detail reported by various system processes. The data in the Appserv Tracing Levels field lists all Application Server tracing levels that are set higher than 0 (zero).

Notes:

- Tracing is logged into the /var/log/dncsLog file on the ISDS.
- Tracing levels set higher than 0 (zero) run the risk of filling up hard drives and slowing system performance.

Important: Unless you are using tracing for a specific reason, we recommend that you set all of your Application Server tracing levels to 0 (zero). Call Cisco Services if you need help setting your Application Server tracing levels.

ISDS Logging Levels

The ISDS Logging Levels field lists all ISDS processes and the level of logging activity that is associated with each process.

System operators can set logging levels for the ISDS processes by clicking **Logging** from the **Utilities** tab of the Administrative Console.

ISDS Processes

The data in the ISDS Processes field lists all the ISDS processes and reports whether those processes are running, or not. Processes that are running are listed as **OK**; processes that are not running are listed as **Error**.

Important: Note the following recommendations regarding other processes that may not be running:

- Check the ISDS for core files.

  Note: The ***Recent ISDS Corefiles (last 2 days)*** (on page 23) field, lists recent ISDS core files.

- If the ISDS has a core file, contact Cisco Services.

  Note: Cisco Services may request that you send them the core file for analysis.

- Use the dncsControl utility to restart the stopped process(s).
- Some processes such as bootpd may not be running, depending on the features that are disabled on the ISDS.

App Server Processes

The data in the App Server Processes field lists all the Application Server processes that are running on the ISDS and reports whether those processes are running, or not.

Note: It may be normal for the orbixd process to show as not running.

Important: Note the following recommendations regarding other processes that may not be running:

- Check the ISDS for core files.
- If the ISDS has a core file, contact Cisco Services.

  Note: Cisco Services may request that you copy the core file and send it to them for analysis.

- Use the appControl utility to restart the stopped process(s).

Recent ISDS Corefiles (last 2 days)

The data in the Recent ISDS Corefiles (last 2 days) field lists any core files saved to the ISDS within the last 48 hours.

Note: A core file indicates that a process on the ISDS failed unexpectedly.

Important: Call Cisco Services if the Recent ISDS Corefiles (last 2 days) section lists any core files. Cisco Services may request that you copy the core file and send it to them for analysis.

Recent App Server Corefiles (last 2 days)

The data in the Recent App Server Corefiles (last 2 days) field lists any core files saved to the Application Server on the ISDS within the last 48 hours.

Note: A core file indicates that a process has failed unexpectedly.

Important: Call Cisco Services if the Recent App Server Corefiles (last 2 days) section lists any core files. Cisco Services may request that you copy the core file and send it to them for analysis.

DNS Check

The data in the DNS Check field reports whether the Domain Name Service (DNS) is running on the ISDS. The system lists **OK** when the DNS is not running; the system lists **Error** when the DNS is running.

Note: Having the DNS enabled on the ISDS may result in communication failures between the ISDS and modulators.

Important: If the DNS is enabled on the ISDS, disable it by editing the **/etc/nssswitch.conf** file so that the **hosts:dns** line reads as **hosts:files**.

Force Tune / Valid Service Check

The data in the Force Tune / Valid Service Check field lists all force-tune service IDs in the system that do not correspond to a valid SAM service. If the Doctor Report lists a service ID that is not associated with a valid service, reconfigure the service ID so that it is associated with a valid service.

ISDS License Check

The data in the ISDS License Check field reveals whether the following ISDS optional features are licensed or unlicensed:

- EAS FIPS Code Filtering
- DOCSIS DHCT Support
- Enhanced VOD Session Throughput
- VOD Session Encryption

Note: These optional features pertain only to sites running SR 2.1 and later system software. Contact Cisco Services to obtain licensing for a feature.

Unused SAM URL Check

The Unused SAM URL Check field provides a warning and a recommendation to run the chkSamUrl utility when the size of the bulk.tbl file is in danger of growing too large. When the bulk.tbl file grows too large, DHCTs may reboot and display a black screen.

ISDS File Size Check

The ISDS File Size Check field lists files 50 MB or larger in the /dvs/dncs/tmp, /var/log, and /tmp directories on the ISDS.

Last Logging Time Stamp for Selected Processes

The Last Logging Time Stamp for Selected Processes field reports the current time and then lists the timestamp associated with the last time the emmDistributor and camAuditor processes wrote to their respective logfiles. System operators can compare the timestamps with the current time to determine whether the emmDistributor and camAuditor processes are running properly.

Note: The timestamp should not be more than a few minutes behind the current time. If you notice that the timestamp associated with the logfiles is more than 15 minutes behind the current time, contact Cisco Services.

DHCT Status Summary

The data in the DHCT Status Summary field provides a status summary of all DHCTs in the database, local and remote sites.

DHCT Type Summary

The data in the DHCT Type Summary field summarizes the number of DHCTs in the database, using each unique combination of DHCT type, revision, OUI, and software table of contents file (if any).

Notes:

- The system also reports the number of DHCTs in the database of type NULL.
- A DHCT of type NULL represents a DHCT that has no record in the database, but has attempted to sign on to the system.

  Important: Call Cisco Services if you have a large number of DHCTs, relative to system size, with a type of NULL.

DHCTs with EMMs Expiring in 15 days

The data in the DHCTs with EMMs Expiring in 15 days field lists the MAC addresses of up to 50 DHCTs in the database that have EMMs set to expire within 15 days.

Notes:

- If the number of DHCTs with EMMs set to expire within 15 days exceeds 50, the system creates a file containing a complete list of those DHCTs.
- The file is called emms.expiring.soon and is found in the /dvs/dncs/Utilities/doctor directory.

Important: Call Cisco Services if you have any DHCTs with EMMs set to expire within 15 days.

EMM Distributor Cycle Summary

The EMM Distributor Cycle Summary field shows data from the emmDistributor process at two moments in time: just prior to the start of a cycle, and then at end of a cycle.

Data pertaining to the start of a cycle (which is actually shown in the second block of output), **EMM Distributor Cycle Start**, lists the parameters that the emmDistributor process is using to calculate the expected cycle duration. Additionally, a summary of the allocation of bridges (and associated DHCT population numbers) to emmDistributor threads, is also displayed.

The second snapshot, **EMM Distributor Cycle Complete**, displays data that was captured as the cycle completes. This data contrasts the expected cycle completion time to the actual cycle completion time.

Download Server Information

The Download Server Information field contains configuration data for each Download Server defined on the system.

Note: This field may not appear if it is not applicable to your configuration.

CVT Configuration Check

The data in the CVT Configuration Check field includes the names and sizes of all of the DHCT image files loaded onto the system. In addition, the CVT Configuration Check field lists all of the DHCT groups that currently have DHCT download assignments.

DHCT counts per 55-1 QPSK

The data in the DHCT counts per 55-1 QPSK field lists the number of DHCTs that communicate with each 55-1 QPSK modulator and demodulator in the system.

Note: This field may not appear if it is not applicable to your configuration.

Sources, Source Definitions and Segments

The data in the Sources, Source Definition and Segments field lists the number of the following items configured on the ISDS:

- Digital Sources
- Encrypted Digital Sources
- Active Source Definitions
- Pending Source Definitions
- Segments
- Encrypted Segments

In addition, the Sources, Source Definition and Segments field flags as an error source IDs that have multiple segments.

Active Subscription Packages

The data in the Active Subscriber Packages field lists the number of active subscriber packages configured on the ISDS.

SI Out-of-band Interval

The SI Out-of-band Interval lists how often out-of-band data is sent to DHCTs.

System Time Message Delivery

If debug flag **+DE** is set for the siManager process, the data in the System Time Message Delivery field confirms whether the system time message (STM) has been sent to DHCTs within the past 12 seconds.

Important: If the Doctor Report reports that STMs are not being delivered every 12 seconds, use the dncsControl utility to restart the siManager process.

PCG Information

The PCG Information field provides configuration data for each PowerKEY® CAS Gateway (PCG) defined on the system.

Timezone and Daylight Savings Time Check

The data in the Timezone and Daylight Savings Time Check field summarizes the time zone and daylight savings time (DST) settings for hubs and DHCTs.

Note: The DHCT Summary section should show **Follow hub** in the columns **Timezone Offset** and **DST Observed**.

Important: If the DHCT Summary section shows **Yes** or **No** in the **DST Observed** column, contact Cisco Services for assistance in configuring all DHCTs to follow the time of the hub to which they belong.

PPV File Check

The PPV File Check field indicates whether the PPVMapFile has been updated with PPV events.

Important: If the Doctor Report indicates an error, call Cisco Services for assistance in making any necessary corrections.

Note: This field may not appear if it is not applicable to your configuration.

GBAM Delivery

Assuming debug flag **+DE** is enabled for the camPsm process, the data in the GBAM Delivery field verifies that time of day (TOD) and purchase GBAMs are delivered.

Notes:

- Purchase GBAMs can be verified only if there are PPV events with an open Buy window.
- Ideally, purchase GBAMs are delivered every 20 seconds and TOD GBAMs every 15 seconds. However, the Doctor Report verifies that these GBAMs have been delivered within the previous 60 seconds.

Important: If the Doctor Report indicates that GBAMs are not being delivered in a timely manner, call Cisco Services.

Note: This field may not appear if it is not applicable to your configuration.

BFS Carousel and OSM Sessions Status

The data in the BFS Carousel and OSM Sessions Status field reports on the status of the BFS carousels and the OSM sessions. The output identifies whether carousels are inband (IB) or out-of-band (OOB), the source ID, the operational status of the carousels, the data rate, the amount of data carried, the indication interval of each carousel, the enabled state, as well as the total time required for each carousel to transmit all its data in one cycle (ACCT).

Additionally, the output lists the aggregate data rate for the inband and out-of-band carousels, which does not include data rates for disabled sources. This field reports for site ISDS as well as any remote site, if applicable.

Important: Refer to *Initial Installation and Upgrade Instructions for the ISDS* (part number 4028676), for the latest data rate recommendations.

BFS Session Status

The data in the BFS Session Status field verifies the following conditions:

- All BFS sources have an active session
- All sessions have a defined source

Important: If a BFS source does not have an active session, or if all sessions do not have a defined source, you have to create them. Call Cisco Services if you need help in creating a session or a source.

Miscellaneous BFS Check

The data in the Miscellaneous BFS Check field verifies the following conditions:

- No more than one dataCarousel process is running for a given BFS source.
- All BFS source definitions are present and are not duplicated.

  Note: If a BFS source definition is not present, the source definition will not be in SI and the DHCT will be unable to tune to that carousel.
- No BFS source is encrypted.

Important: Refer to *Initial Installation and Upgrade Instructions for the ISDS* (part number 4028676), or your appropriate upgrade installation instructions for assistance in setting data rates.

Ping All Active Elements

The data in the Ping All Active Elements field reports whether the communication path between the ISDS and the following system devices is active:

- QAM modulator (if applicable)
- QPSK modulator (if applicable)
- PCG
- TED

Important: If the Doctor Report reports an error, complete the following tasks to troubleshoot the error:

- Visually check that the device is powered on and that the cabling is secure.

- Use a network analyzer to confirm that IP traffic is reaching the device.
- Reboot the device.

DoctorRemote

The Doctor Report reports on the configuration of any remote site supported by the system. The information collected from remote sites is similar to the information collected from the ISDS. The following list contains the fields reported on for the remote sites:

- System Name
- All SAI Installed Package Information
- LIONN Info
- Virtual CPUs
- Physical Memory Configuration
- IO Devices
- Disk Info
- Checking the Status of the Metadevices
- LIONN Disk Partition Utilization
- LIONN Swap Space
- LIONN Basic System Performance Stats
- LIONN Database Log Check

  Note: This field appears only for remote sites. The LIONN Database Log Check field reports on the size of the /dvs/lionndb/liondb.log and /dvs/lionndb/lionnconnection.log files.
- LIONN Database Process Check

  Note: This field appears only for remote sites. The LIONN Database Process Check field reports on whether the Informix daemon processes are running.
- LIONN Load Average
- Current LIONN Debug Flags Set
- LIONN Processes
- Recent LIONN Corefiles (last 2 days)
- DNS Check
- Force Tune / Valid Service Check
- LIONN File Size Check

- Timezone and Daylight Savings Time Check
- EUT Update Check
- Ping All Active Elements

3

Backup Recommendations

Introduction

This chapter provides recommendations for the frequency with which system operators should back up the data of their ISDS. 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 ISDS 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 ISDS. Use the information in this chapter for tape selection and tape cleaning recommendations.

In This Chapter

System Backup Frequency

System operators can ensure the integrity of their 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.

Full System Backup

A full system backup refers to a backup of the file systems and the database.

System operators should perform a complete system backup prior to making any substantial modification to the system.

In addition, system operators should perform a complete system backup just prior to upgrading to new system software, as well as right after the upgrade. The backup just prior to the upgrade will be used in case of a major hardware failure.

Important: Clearly label the backup tapes and remove them from the working area for safe keeping. New and old backups are not compatible.

Informix Database Backup

The Informix database contains all headend configuration information, as well as data needed to provision and authorize Digital Home Communication Terminals (DHCTs). System operators should perform a complete backup of the Informix database once a day. In addition, system operators should perform a complete backup of the database immediately before and after a channel lineup change or a major system configuration change.

File System Backup

System operators should perform a complete backup of the ISDS and Application Server file systems once a week.

Important: You can back up the file system of the ISDS without first shutting down the system components. However, our engineers highly recommend that you schedule your file system backups for periods of lowest system activity.

Key Files Backup

The key files need to be backed up only as part of a system upgrade.

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 ISDS or Download Server.
- You can purchase 4-mm tapes or 8-mm tapes in various lengths. Refer to the following chart, compiled by our 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	4000000	16
8 mm	112	5/10	10000000	32
8 mm	160	7/14	14000000	128
4 mm DDS	90	2/4	4000000	16
4 mm DDS-2	120	4/8	8000000	32
4 mm DDS-3	125	12/24	24000000	128
4 mm DDS-4	150	20/40	40000000	128
4 mm DAT72	170	36/72	72000000	128

- Buy the largest tapes that your tape drive supports.

  Example: Buy 170m DAT72 tapes if you have a DAT72 tape drive; buy 150m DDS-4 tapes if you have a DDS-4 tape drive.

- The backup scripts detect what tape drive your system uses and supplies default parameters in preparation of running the scripts. The operator can override the default values, at the command line, if desired.
- 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 use. 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.

4

Backing Up and Restoring the Informix Database

Introduction

The Informix database contains all headend configuration information, as well as data needed to provision and authorize DHCTs. Our engineers recommend 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 ISDS in order to back up your Informix database. All system components can be running while you back up the database.

In This Chapter

Database Backup and Restore

The Informix database contains all headend configuration information, as well as data needed to provision and authorize set-tops. In the event of a power failure, for instance, you might need to restore the database. Only through regular daily backups of your database can you ensure the integrity and persistence of your system data.

Recommendations

Consider the following recommendations before you backup and restore your Informix database.

ISDS Recommendations

We strongly recommend that you connect the ISDS to an Uninterruptible Power Supply (UPS) to prevent unexpected and abrupt power failures of the ISDS.

Database Backup Script Options

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

- *-b* — block size. Specifies the blocksize that should be used, in Kilobytes.
- *-l* — Local-tape-drive. Specifies tape drive to use on local host computer. (for example — /dev/rmt/0h)
- *-v* — verbose. Verbose output.
- *-s* — tape size. Specifies the tape size that should be used, in Kilobytes.
- *-t* — tape label. Backup tape label. This must be a unique string with no spaces.
- *-h* — help. Provides a brief description of the valid options.

Database Backup Recommendations

Consider the following recommendations when you backup your database.

- We strongly recommend that you backup your database once each day, preferably early in the morning or late at night, when system activity is usually at a minimum.
- Avoid backing up your database while you are performing any of the following system tasks:
  - Running the Interactive Program Guide (IPG) Collector
  - Loading an Entitlement Management Message (EMM) DVD

  - Staging Set-Tops

- To back up the Informix database, you must have a tape drive connected to or included in your system. Some platforms contain internal tape drives; others must use external tape drives.
- You do not have to shut down the ISDS or the Download Server to back up your Informix database. All system components can be running while you back up the database.
- It can take up to 30 minutes to back up a typical database with approximately 100,000 set-tops. Larger systems may take longer.

Restore Recommendations

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

Backup Tape Recommendations

Consider the following recommendations concerning your tape drives and the tapes that you use for the database backup.

- Use seven tapes (or sets of tapes) for the database backup, one for each day of the week.

  Important: The tapes that you use to back up your Informix database wear out over time. Be sure to replace your tapes at least once a year.

- You can back up your Informix database 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 ISDS. An 8-mm tape is too big for a 4-mm tape drive; a 4-mm tape is too small for an 8-mm tape drive. Ask the person who handles your account if you are not sure which type of tape is appropriate for your system.
- You can purchase 4-mm tapes or 8-mm tapes in various lengths. While all tapes wear out over time, a longer tape is likely to wear out quicker than a shorter tape because the strength of a tape is inversely proportional to the length of the tape. Use the following guidelines when you purchase tapes to back up your Informix database:

  - 4-mm tapes: Do not exceed 150 meters
  - 8-mm tapes: Do not exceed 160 meters

- Depending on the size of your database, you may need more than one tape to do a complete backup. If you need more than one tape to back up your database, the backup script will prompt you to remove the existing tape and to insert a new tape at the appropriate time.
- The script used by the ISDS to back up the Informix database uses the following default tape drive configuration:

- Tape size: 5859375 KB
- Block size: 16
- Device name: /dev/rmt/0h

- This tape drive configuration is in use on a majority of systems. Occasionally, 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.

Tape Drive Configuration

Checking Your Tape Drive Configuration

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

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. Open an xterm window as root user.
2. Make sure 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 (0-7) possible tape drive configurations and displays the results.
4. Examine the results and use the following observations to determine the device name of your tape drive.
   - If no tape drives are detected in /dev/rmt/0 through /dev/rmt/7, the results show No such file or directory. Therefore, you can conclude that the system did not detect any tape drives. You should investigate why a tape drive was not detected.
   - If a tape drive is detected in /dev/rmt/0, for example, the system should accurately note that no tape is loaded in /dev/rmt/0. 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. Record the device name of your tape drive.

   Note: You might need to refer to this device name when you back up or restore the database.
6. Type **exit** and press **Enter** to close the xterm window.

Back Up the Database

In this procedure, you will back up the Informix database. The system release DVD should still be in the DVD drive of the ISDS.

Backing Up the ISDS Database

Use this procedure to back up the ISDS database.

Notes:

- The ISDS 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 ISDS.

2 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**.

3 Type **df -n** and then press **Enter**. A list of the mounted filesystems appears.

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

4 After waiting at least 1 minute, did **/cdrom/cdrom** appear in the output of the command executed in step 3?

- If **yes**, go to step 5.
- If **no**, follow these instructions.
  - **a** Type **/etc/init.d/volmgt stop** and then press **Enter**.
  - **b** Type **/etc/init.d/volmgt start** and then press **Enter**.
  - **c** Repeat step 3.

5 Label your backup tape with the following information:

ISDS Database Backup [Day of the Week]

[Site Name]

[Software Version]

System Release DVD x.x.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.

6 Insert the tape into the tape drive of the ISDS and wait until the green light stops flashing.

7 Type **. /dvs/dncs/bin/dncsSetup** and then press **Enter**. The system establishes the root user environment.

Important: Be sure to type the dot, followed by a space, prior to typing /dvs.

8 Choose one of the following options.

- If you are using the standard tape drive configuration, follow these instructions.
  - **a** Type **/cdrom/cdrom0/s3/backup_restore/backupDatabase** and then press **Enter**. The system displays the following message:

    Please mount tape 1 on /dev/rmt/0h and then press Return to continue.
  - **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/backupDatabase -b [blocksize] -s [tapesize] and then press **Enter**.

Note: Substitute the blocksize and tapesize that pertain to your system for [blocksize] and [tapesize].

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.

10 Press **Enter**. 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.

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

12 Remove the DVD and tape(s) and store them in a safe place.

13 Type **exit** and then press **Enter** to log out the root user.

Restore the Database

This section contains procedures for restoring the database from your backup tapes.

Restore Recommendations

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

How Many Tapes Are in the Backup?

You may have used 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*** (on page 44) 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*** (on page 45) procedure to restore the database.

Restoring the Informix Database Using One Backup Tape

Complete the following steps to restore the ISDS and Download Server databases using only one backup tape.

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

Important:

- The ISDS and Application Server must be stopped before you restore the database.
- Be sure your tape is write-protected before you use it to restore the database.

1 If necessary, open an xterm window on the ISDS.

2 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**.

3 Have you just restored the ISDS file system?

- If **yes**, go to step 4.
- If **no**, go to step 5.

4 Complete the following steps. (You have just restored the ISDS file system.)

a Type **. /dvs/dncs/bin/dncsSetup** and then press **Enter**. The system establishes the root user environment.

Important: Be sure to type the dot, followed by a space, prior to typing /dvs.

b Type **/export/home/informix/bin/formatDbSpace.sh** and then press **Enter**. The system formats the database partitions.

5 Insert the system release DVD into the DVD drive of the IPTV Services Delivery System.

6 Type **df -n** and then press **Enter**. A list of the mounted filesystems appears.

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

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

8 Type **/cdrom/cdrom0/s3/backup_restore/restoreDatabase -v** and then press **Enter**.

9 When the **Is there more than 1 tape in this backup? [Y/N]** message appears, type **n** and then press **Enter**. The system displays a message about ensuring that the backup tape is in the drive.

10 Press **Enter**. The system restores the database.

11 When the **Successfully restored the database** message appears, remove the tape and store it in a safe place.

12 Complete the following steps to eject the DVD.

a Type **cd /** and then press **Enter**.

b Type **/etc/init.d/informix stop** and then press **Enter**. The system stops the Informix oninit processes.

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

d Type **/etc/init.d/informix start** and then press **Enter**. The system restarts the Informix oninit processes.

13 Remove the DVD and store it in a safe place.

14 Type **exit** and then press **Enter** to log out the root user. You can now restart the ISDS and Application Server.

Restoring the Informix Database Using More Than One Backup Tape

Complete the following steps to restore the ISDS and Download Server databases 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:

- The ISDS and Application Server must be stopped before you restore the database.
- Be sure your tapes are write-protected before you use them to restore the database.

1 If necessary, open an xterm window on the ISDS.

2 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**.

3 Have you just restored the ISDS file system?

   - If **yes**, go to step 4.
   - If **no**, go to step 5.

4 Complete the following steps. (You have just restored the ISDS file system.)

   a Type **. /dvs/dncs/bin/dncsSetup** and then press **Enter**. The system establishes the root user environment.

   Important: Be sure to type the dot, followed by a space, prior to typing /dvs.

   b Type **/export/home/informix/bin/formatDbSpace.sh** and then press **Enter**. The system formats the database partitions.

5 Insert the system release DVD into the DVD drive of the IPTV Services Delivery System.

6 Type **df -n** and then press **Enter**. A list of the mounted filesystems appears.

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

7 Type **/cdrom/cdrom0/s3/backup_restore/restoreDatabase -v** and then press **Enter**.

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

9 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.

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

11 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.

12 Type **y** and then press **Enter**. The **Do you want to back up the logs? (y/n)** message appears.

13 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.

14 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.

15 Repeat step 14 for as many backup tapes that are in the backup series.

16 When the **Restore a level 1 archive? (y/n)** message appears, type **n** and then press **Enter**.

17 When the **Do you want to restore log tapes? (y/n)** message appears, type **n** and then press **Enter**.

18 When the **DNCS Informix partition restore completed and verified** message appears, remove the final tape and store it in a safe place.

19 Complete the following steps to eject the DVD.

a Type **cd /** and then press **Enter**.

b Type **/etc/init.d/informix stop** and then press **Enter**. The system stops the Informix oninit processes.

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

d Type **/etc/init.d/informix start** and then press **Enter**. The system restarts the Informix oninit processes.

20 Remove the DVD and store it in a safe place.

21 Type **exit** and then press **Enter** to log out the root user. You can now restart the ISDS and Application Server.

5

Backing Up and Restoring the ISDS

Introduction

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

Important: You can back up the file system of the ISDS without first shutting down the system components. However, our engineers highly recommend that you schedule your file system backups for periods of lowest system activity.

In This Chapter

Back Up the File Systems

The upgrade scripts do not back up the ISDS file systems. Prior to beginning the upgrade, back up the file systems manually. The following procedures provide instructions on backing up the file systems of the ISDS.

Note: The file system backup may require more than one tape.

Backup Considerations

Before backing up the file system, our engineers recommend that system operators first check the dncs and root user e-mail accounts on the system to be backed up. The e-mail accounts will reveal whether any metadevice errors exist.

Recommended Frequency

Our engineers recommend that system operators perform a complete system backup at least once a month, just prior to upgrading to new system software, as well as after the upgrade.

Filesystem 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. (for example — /dev/rmt/0h)
- *-v* — verbose. Verbose output.
- *-t* — tape label. Backup tape label. This must be a unique string with no spaces.
- *-h* — help. Provides a brief description of the valid options.

Using the tar Utility

If you need to back up the key files from a remote computer, you can use the tar utility to create a tape archive instead of using the backupFileSystems script.

Failure of File System Backups and the Real-Time, Class Process

Occasionally, the file system backup may fail. If the backup fails, system operators should check whether there are any real-time, class processes that are running. Current file system backup scripts can handle only the ntpd process that is running as a real-time class process.

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 complete the following steps to see if any real-time, class processes are running.

1 From an xterm window, type **ps -efc | grep RT** and then press **Enter**. The system reports whether any real-time, class processes are running on that device.

2 Are any real-time, class processes running (other than the ntpd process)?

- If **yes** (and the file system backup still failed), call Cisco Services for assistance.
- If **no**, re-run the procedures to back up the file system. If the backup still fails, call Cisco Services.

Preparing for the File System Backup

Follow this procedure to prepare for the ISDS file system backup.

1 If necessary, open an xterm window on the ISDS.

2 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**.

3 Insert the system release DVD into the DVD drive of the ISDS.

4 Type **df -n** and then press **Enter**. A list of the mounted filesystems appears.

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

5 After waiting at least 1 minute, did **/cdrom** appear in the output of the command executed in step 4?

- If **yes**, go to step 6.
- If **no**, follow these instructions to stop and restart the vold process, which manages the auto-mount functions for the DVD drive.
  a Type **/etc/init.d/volmgt stop** and then press **Enter**.
  b Type **/etc/init.d/volmgt start** and then press **Enter**.
  c Repeat step 4.

6 Label a blank tape with the following information:

ISDS File System Backup [Date]

[Site Name]

[Software Version]

System Release x.x.x DVD

Notes:

- Customize the date, site name, and software version for the site you are backing up.
- The file system backup may require more than one tape.

Backing Up the File System of the IPTV Services Delivery System

Follow these instructions to back up the file system of the ISDS.

Notes:

- If you have correctly followed the directions in this chapter, you should be logged in to an xterm window as root user.
- Expect to spend about an hour backing up the IPTV Services Delivery System.

1. Insert the blank tape into the tape drive of the IPTV Services Delivery System and wait for the green light to stop flashing.
2. Type **./dvs/dncs/bin/dncsSetup** and then press **Enter**. The system establishes the root user environment.
3. Type **/cdrom/cdrom0/s3/backup_restore/backupFileSystems** and then press **Enter**.

   Result:

   - The system backs up the IPTV Services Delivery System file system.
   - If the backup requires more than one tape, the system will prompt for the next tape. Insert a new tape and continue the backup.

     Note: If more than one tape is required, be sure to include the tape number on the label. Label the first tape generated by the backup with the number 1.
   - The system displays a message when the backup is complete.
4. When the backup is complete, remove the tape and store in a safe place.
5. Type **exit** and then press **Enter** to log out the root user.

Back Up the Key Files

Overview

Consider the following points about backing up the key files of the ISDS.

Recommended Frequency

The key files consist of those files required to boot the ISDS. 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.

Key Files Backup Script Options

The script that backs up the 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)
- *-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 ISDS key files at the same time, be sure to specify different directories for each set of key files, or the backups will overwrite each other.
- *-v* — verbose. Verbose output
- *-A* — Alternate Root Directory. Specify the Alternate Root Directory where the key files should be restored. This is useful during a Live Upgrade (System Release DVD upgrades) when you may want to back up key files from one root directory and restore them to another root directory. The Alternate Root Directory must contain the /usr/sbin/tar directory, or the backup script will fail to execute correctly.
- *-h* — help. Provides a brief description of the valid options.

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.
- The backupKeyFiles script currently does not support the *–E* option.

Preparing for the Key Files Backup

Complete the following steps to prepare to back up the key files.

1. If necessary, open an xterm window on the ISDS.
2. 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**.
3. Insert the system release DVD into the DVD drive of the IPTV Services Delivery System.
4. Type **df -n** and then press **Enter**. A list of the mounted filesystems appears.

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

   [ISDS] Key Files Backup [Date]
   [Site Name]
   [Software Version]
   System Release DVD x.x..x

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

Backing Up the Key Files

Complete the following steps to back up the key files.

Note: You should be logged in to an xterm window as root user.

1. Insert the blank tape into the tape drive of the server you are backing up, and wait for the green light to stop flashing.
2. Type **/cdrom/cdrom0/s3/backup_restore/backupKeyFiles -v** and then press **Enter**. The system backs up the ISDS, Download Server, or LIONN 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 DVD and store it in a safe place.

Restore the File System

Overview

Consider the following points about restoring the file system of the ISDS.

Prerequisite

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

Important: Be sure your tape(s) are write-protected before you use them to restore the system.

File System Restore Script Options

The script that restores the ISDS file systems 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)
- *-B* – Backup directory. Specifies the directory that contains the backup from which the file system will be restored. The backup directory must be on an NFS-mounted filesystem.
- *-v* — verbose. Verbose output
- *-i* — interactive. Runs the restoration script in interactive mode
- *-h* — help. Provides a brief description of the valid options

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

Preparing to Restore the File System

Complete the following steps to prepare to restore the file system.

Important: You need to know the IP address and the netmask of the IPTV Services Delivery System in order to complete this procedure.

1. Open an xterm window on the ISDS.
2. 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**.
3. Insert the system release DVD into the DVD drive of the IPTV Services Delivery System.

4 Is the server a SUN T5440?

- If **yes**, you need to set the output and input devices to virtual-console. Go to step 5.
- If **no**, go to step 8.

5 Type **eeprom output-device=virtual-console** and press **Enter**. The output device is set to virtual console.

6 Type **eeprom input-device=virtual-console** and press **Enter**. The input device is set to virtual console.

7 Complete the following steps to connect the ILOM serial management port:

a Connect a laptop computer to the serial management port of the server.

b Start the HyperTerminal application on the laptop so that it can communicate with the server. Configure the application with the following parameters:

- Baud rate=9600
- Data bits=8
- Parity=none
- Stop bit=1
- Flow control=no

c From the login prompt on the terminal, log on using **root** as the username and enter the password when prompted.

Note: The default password for root is **changme**.

d Type **start /SP/console** and press **Enter**. The system console is started. The console window will be used as the screen, and the keyboard connected to the ISDS will be the input device when you start the system in single user mode.

8 Type **shutdown -y -g0 -i0** and then press **Enter**. The system halts all processes on the ISDS, and an **ok** prompt appears.

9 At the ok prompt on the server into which you have inserted the DVD, type **boot cdrom - SAshell** and then press **Enter**. The system 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.

10 In the process of booting, did the Solaris Installation menu appear?

- If **yes**, go to step 7.
- If **no** (the system successfully found the configuration information it needed), go to step 8.

11 Complete the following steps on the Solaris Installation menu.

- **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 ISDS and then select **Continue**.
- **d** At the IP Address menu, type the IP address of the ISDS 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 ISDS 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**. 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**. 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**. An xterm window opens.

12 Insert your most recent file system backup tape into the tape drive of the server you are restoring. If the file system backup exists on more than one tape, insert tape number 1.

13 Type **cd /tmp/cdrom/backup_restore** and then press **Enter**. The /tmp/cdrom/backup_restore directory becomes the working directory.

14 Go to *Restoring the File System* (on page 57).

Restoring the File System

Complete the following steps to restore the file system of the ISDS.

1 If necessary, open an xterm window on the ISDS and log in as root user.

2 Type **./restoreFileSystems -v** and then press **Enter**.

Result:

- The system restores the ISDS file system.
- If the backup required more than one tape, the system prompts for the next tape. Insert the next tape and continue the restoration.
- The system displays a message when the restoration is complete.

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

4 Is the server a SUN T5440?

- If **yes**, you need to restore the output and input devices. Go to step 5.
- If **no**, go to step 7.

5 Type **eeprom output-device=screen** and press **Enter**. The output device is set to virtual console.

6 Type **eeprom input-device=keyboard** and press **Enter**. The input device is set to virtual console.

Note: The monitor and keyboard will be used as the output and input devices after the next reboot.

7 Type **/usr/sbin/shutdown -y -i0 -i6** and then press **Enter**. The ISDS reboots and the Common Desktop Environment (CDE) login window appears.

Note: The system may reboot a few times as part of the restoration process.

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

9 Follow the ***Restore the Database*** **(on page 44)** procedures to restore the Informix database. After restoring the Informix database, go to step 7 to enable disk mirroring.

10 Type **/cdrom/cdrom0/s3/backup_restore/mirrState -a** and then press **Enter**.

Note: The latest System Release DVD should still be in the drive of the ISDS and you should still be logged in as root user to an xterm window.

The system displays the following message:

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

11 Type **y** and then press **Enter**. The system enables the disk mirroring functions on the ISDS.

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

12 Type **eject cdrom** and then press **Enter**. The system ejects the DVD.

13 Click the right mouse button on the server you restored and select **Log Out**. The root user logs off and the CDE window returns.

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

Restore the Key Files

Overview

Consider the following points about the restoration of the 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.

Key Files Restore Script Options

The script that restores the 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)
- *-v*—verbose. Verbose output
- *-h*—help. Provides a brief description of the valid options

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

Complete the following steps to prepare to restore the key files.

1. If necessary, open an xterm window on the ISDS.
2. 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**.
3. Insert the latest System Release DVD into the DVD drive of the ISDS.
4. Type **df -n** and then press **Enter**. A list of the mounted filesystems appears.

   Note: The presence of /cdrom in the output confirms that the system correctly mounted the DVD.
5. Insert your most recent key files backup tape into the tape drive of the ISDS, and wait for the green light to stop flashing. Go to ***Restoring the Key Files on the ISDS*** (on page 60).

Restoring the Key Files on the ISDS

Complete the following steps to restore the key files of the ISDS.

1. If necessary, open an xterm window on the ISDS and log in as **root** user.
2. Type **/cdrom/cdrom0/s3/backup_restore/restoreKeyFiles -v** and then press **Enter**. The system restores the key files and displays a message when the restoration is complete.
3. When the restoration is complete, eject the tape and store it in a safe place.
4. Type **eject cdrom** and then press **Enter**.
5. Remove the DVD and store it in a safe place.
6. On the ISDS, type **/usr/sbin/shutdown -y -g0 -i6** and then press **Enter**. The ISDS reboots.
7. Log on to the CDE of the ISDS as a **dncs** administrator.

6

Prerequisites for Overall System Checks

Introduction

This chapter outlines prerequisites for overall system checks. Before you refer to the overall system checks in ***Overall System Checks*** (on page 67), complete the following prerequisite steps:

- Enable Logging
- Enable cmd2000 Listener
- Check Automated Scripts

In This Chapter

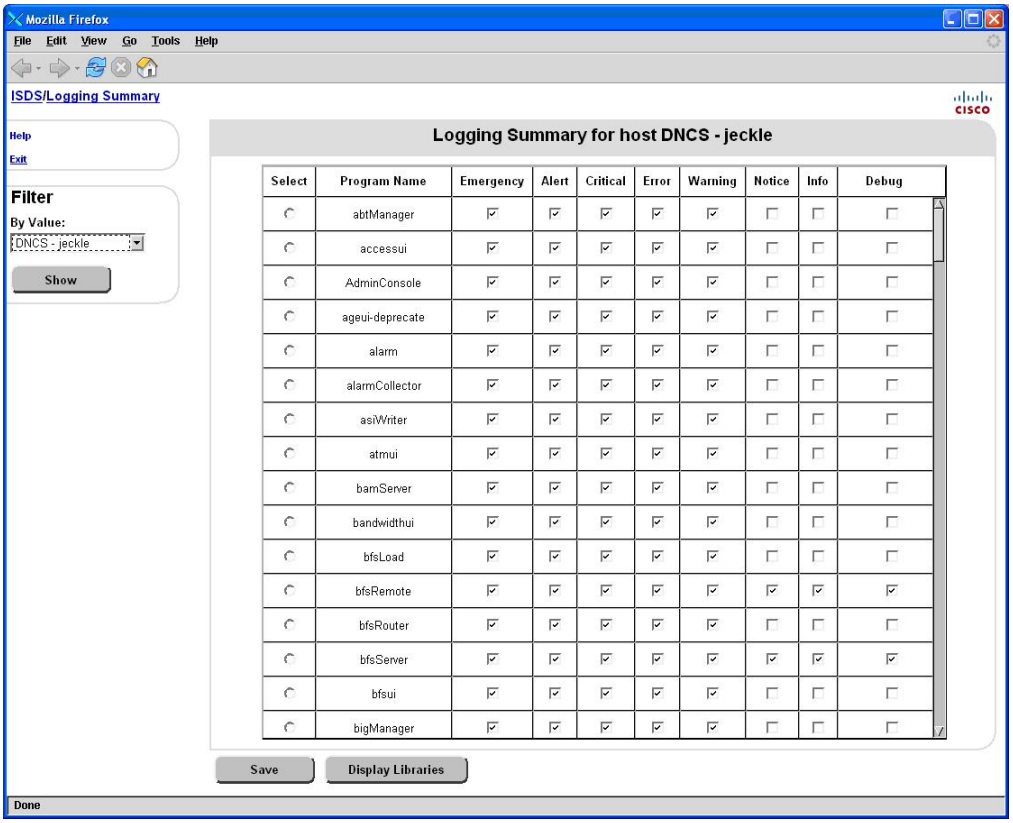
Enabling Logging

You can use the Logging Summary window to enable logging and set logging levels for various ISDS processes.

Important: If you set your logging levels too high, you could raise your ISDS load levels to unacceptable levels. You should only adjust these logging levels if you are troubleshooting a specific problem.

1 From the ISDS Administrative Console, select the **ISDS** tab, and then select the **Utilities** tab.

2 Click **Logging**. The Logging Summary window opens.



3 Scroll down until the process you want to check comes into view.

4 To the right of the process, select the desired logging level.

5 Repeat steps 3 and 4 for each logging level you want to change.

6 When you have finished making changes, click **Save** and then **Exit** to save your changes and close the Logging Summary window.

Using the logLvl Utility

You can also use the logLvl utility to view and change logging levels from a command line in the /export/home/dncs directory. The following commands are available:

Command	Result

logLvl	Displays the current logging level for all processes.
	`/export/home/dncs>logLvl`
	`abtManager +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP`
	`accessui +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP`
	`AdminConsole +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP`
	`.`
	`.`
	`.`

logLvl <processname>	Displays the current logging level for the specified process.
	`/export/home/dncs>logLvl siManager`
	`siManager +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP`

logLvl <processname> +<level>	Turns on a logging level for the specified process.
	`/export/home/dncs>logLvl siManager +NO`
	`siManager +EM +AL +CR +ER +WA +NO -IN -DE -PE -PI -ZIP`

logLvl <processname> -<level>	Turns off a logging level for the specified process.
	`/export/home/dncs>logLvl siManager -NO`
	`siManager +EM +AL +CR +ER +WA -NO -IN -DE -PE -PI -ZIP`

logLvl -h	Provides a help output for the logLvl utility.

Enabling and Starting cmd2000 Listener

Listen Mode Details

When the cmd2000 process is in listen mode, it can be used to collect reboot information. When a set-top reboots, it sends information that cmd2000 can read if it is running. This information is saved to a log file and analyzed later to determine the cause of reboots.

Check To See If cmd2000 Is Running

If you need to check whether cmd2000 is running, use the command **ps -ef | grep cmd2000**. If cmd2000 is already running, the ISDS will return a message that looks like the following:

```
jeckle1:/dvs/dncs/Utilities/doctor>ps -ef|grep cmd2000
dncs 21620 7943 0 09:45:25 pts/3 0:00 grep cmd2000
dncs 21361 7943 0 09:45:19 pts/3 0:00 cmd2000 -log -listen -nostdin
```

If cmd2000 is **not** already running, the ISDS will return a message that looks like the following:

```
jeckle1:/dvs/dncs/Utilities/doctor>ps -ef|grep cmd2000
dncs 20991 7943 0 09:44:42 pts/3 0:00 grep cmd2000
```

New Method for Running cmd2000 in Listen Mode

You can use the following command to run cmd2000 in listen mode:

nohup cmd2000 -log -listen -nostdin 2>/dev/null &

Checking Automated Scripts

Review all automated scripts to ensure that all scripts that should be running are running. In addition, review scripts to ensure you do not have any site-specific scripts that are no longer being used.

Important: Some slight variations in the scripts listed will exist based on your specific hardware versions.

You can complete these steps to check the automated scripts for different users.

1. Log into the desired machine as the user you want to check. For example, to check automated scripts for the root user on the ISDS, log into the ISDS as **root** user.
2. Type **crontab -l** and press **Enter.** The automated scripts for the user login are listed.

   Note: The character in the above command is the letter "l," not the number 1.
3. Compare the list of automated scripts with the appropriate list.

   Important: Any scripts that are preceded by a # symbol will not be executed. The # symbol notation disables a script.
4. Add or remove scripts as necessary. If you need help locating or adding a script, contact Cisco Services.

7

Overall System Checks

Introduction

This chapter provides checklists for items you should check to ensure your system continues to operate as expected.

In This Chapter

Checking the Health of your Overall System

The following checklists provide objectives you should monitor to ensure the health of your system. The checklists are organized as follows:

- Doctor Report checks to be performed twice daily
- Additional checks to be performed twice daily
- Doctor Report checks to be performed once daily
- Additional checks to be performed once daily
- Checks to be performed weekly
- Checks to be performed at other times

Important: While we recommend that you run the Doctor Report twice daily (morning and evening), you should always run the Doctor Report anytime you suspect or experience problems.

The items in the Additional Checks lists cannot be performed using the Doctor Report.

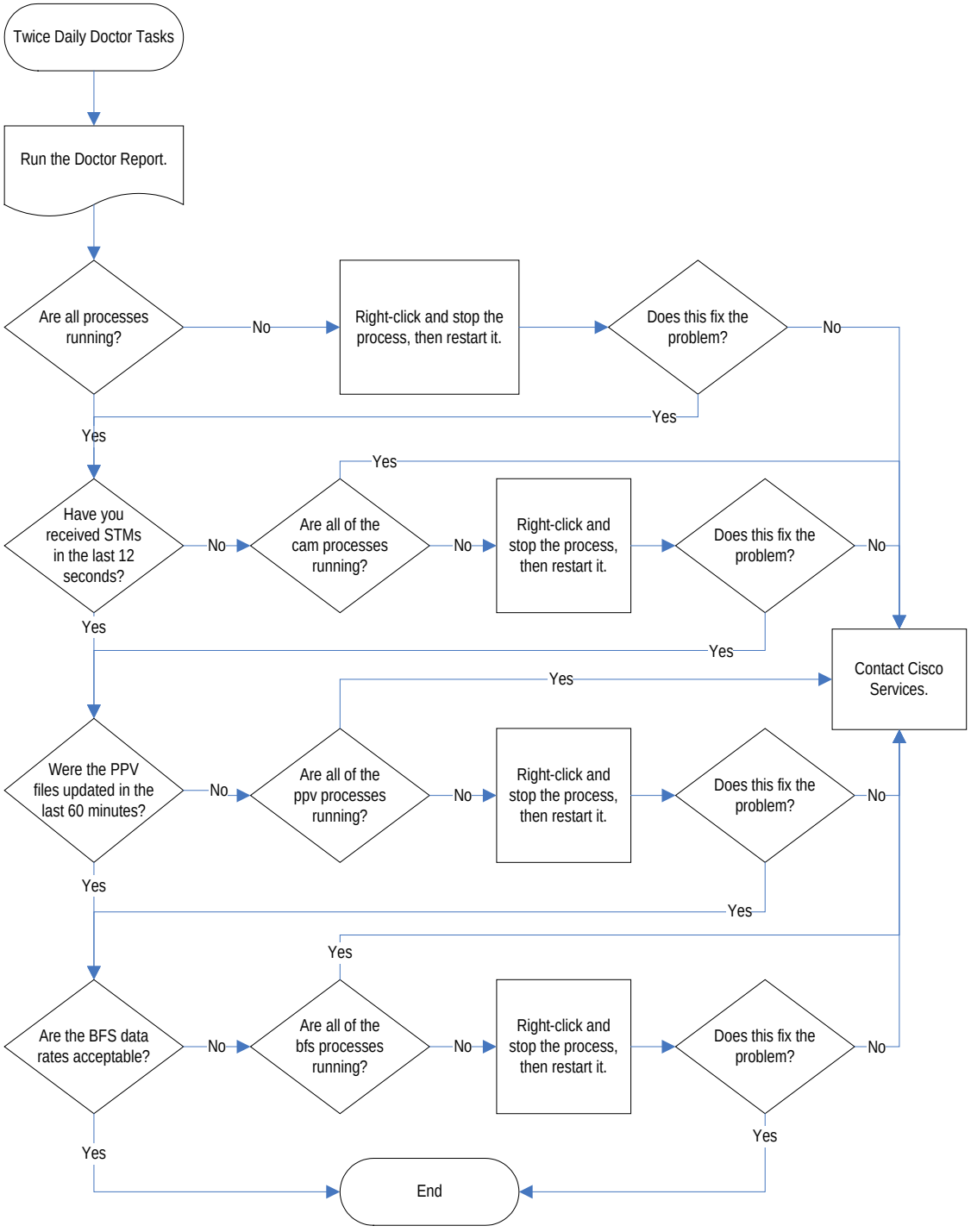
CAUTION:

Before you undertake any of the procedures, you must verify that the subscriber's service will not be affected. If the procedure causes any sort of service interruption, you must perform it during a maintenance window.

Doctor Report Checks - Perform Twice Daily

Date:_____First Check Time:_____Second Check Time:_____

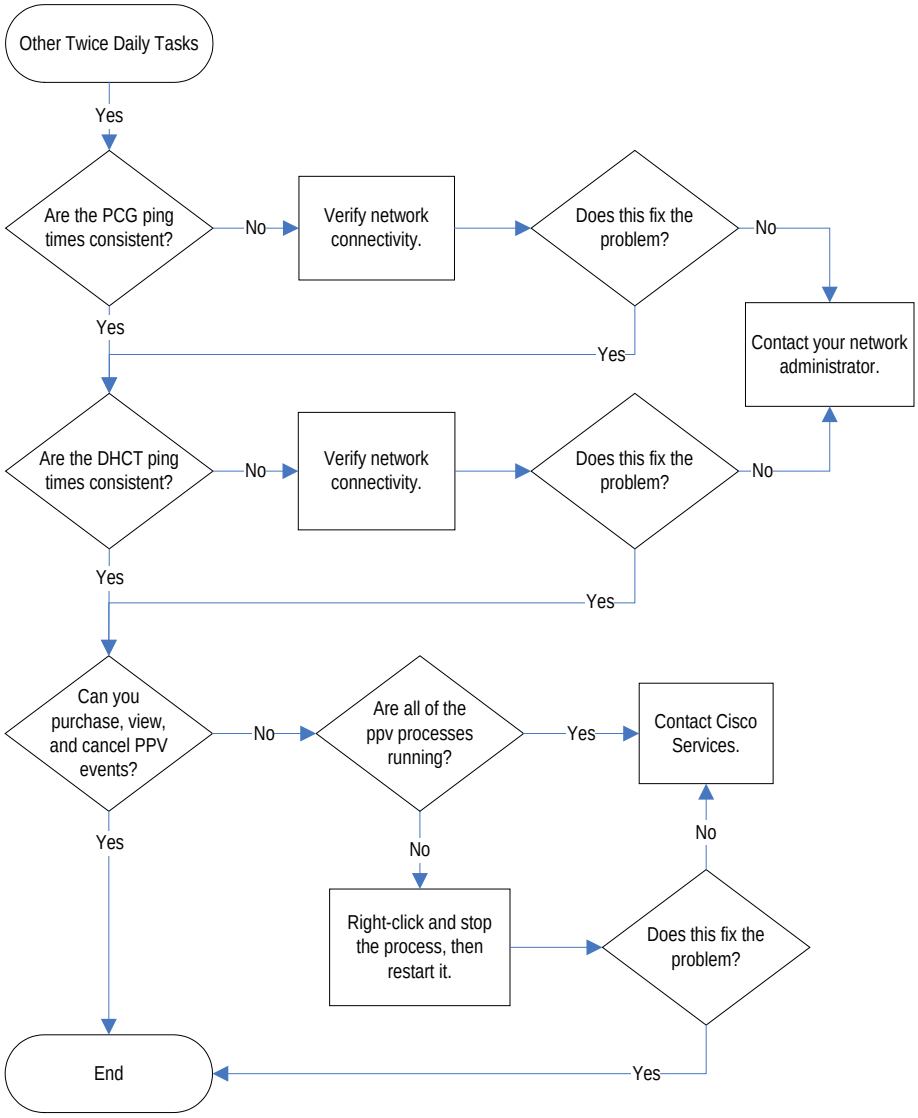
Objective	Tips	Passed?	Passed?
All ISDS processes are running.	saManager does not usually run on systems with Aptiv Digital Application Servers.	☐ Yes ☐ No	☐ Yes ☐ No
All App Server processes are running.	Does not apply to systems with third-party Application Servers.	☐ Yes ☐ No	☐ Yes ☐ No
System Time Messages (STMs) were delivered within the last 12 seconds.	Does not apply to systems with third-party Application Servers.	☐ Yes ☐ No	☐ Yes ☐ No
PPV files were updated within the last 60 minutes.	Does not apply to systems with third-party Application Servers.	☐ Yes ☐ No	☐ Yes ☐ No
The EUT (Entitlement Unit Table) was updated within the last 60 minutes.	The EUT lists all EIDs (packages) associated with every source in the system. If the information in the EUT is wrong, subscribers cannot tune to channels they are authorized to receive.	☐ Yes ☐ No	☐ Yes ☐ No
BFS Checks: ■ All BFS carousels are up. ■ Sessions are active. ■ Only 1 process per carousel. ■ BFSDir updated within the last 60 minutes.	Make sure all data rates are under their recommended maximums.	☐ Yes ☐ No	☐ Yes ☐ No


Twice Daily Doctor Tasks
Run the Doctor Report.
Are all processes running?
No
Right-click and stop the process, then restart it.
Does this fix the problem?
No
Yes
Yes
Have you received STMs in the last 12 seconds?
No
Are all of the cam processes running?
No
Right-click and stop the process, then restart it.
Does this fix the problem?
No
Yes
Yes
Yes
Contact Cisco Services.
Were the PPV files updated in the last 60 minutes?
No
Are all of the ppv processes running?
No
Right-click and stop the process, then restart it.
Does this fix the problem?
No
Yes
Yes
Yes
Are the BFS data rates acceptable?
No
Are all of the bfs processes running?
No
Right-click and stop the process, then restart it.
Does this fix the problem?
No
Yes
Yes
End

Additional Checks - Perform Twice Daily

Date:_____First Check Time:_____Second Check Time:_____

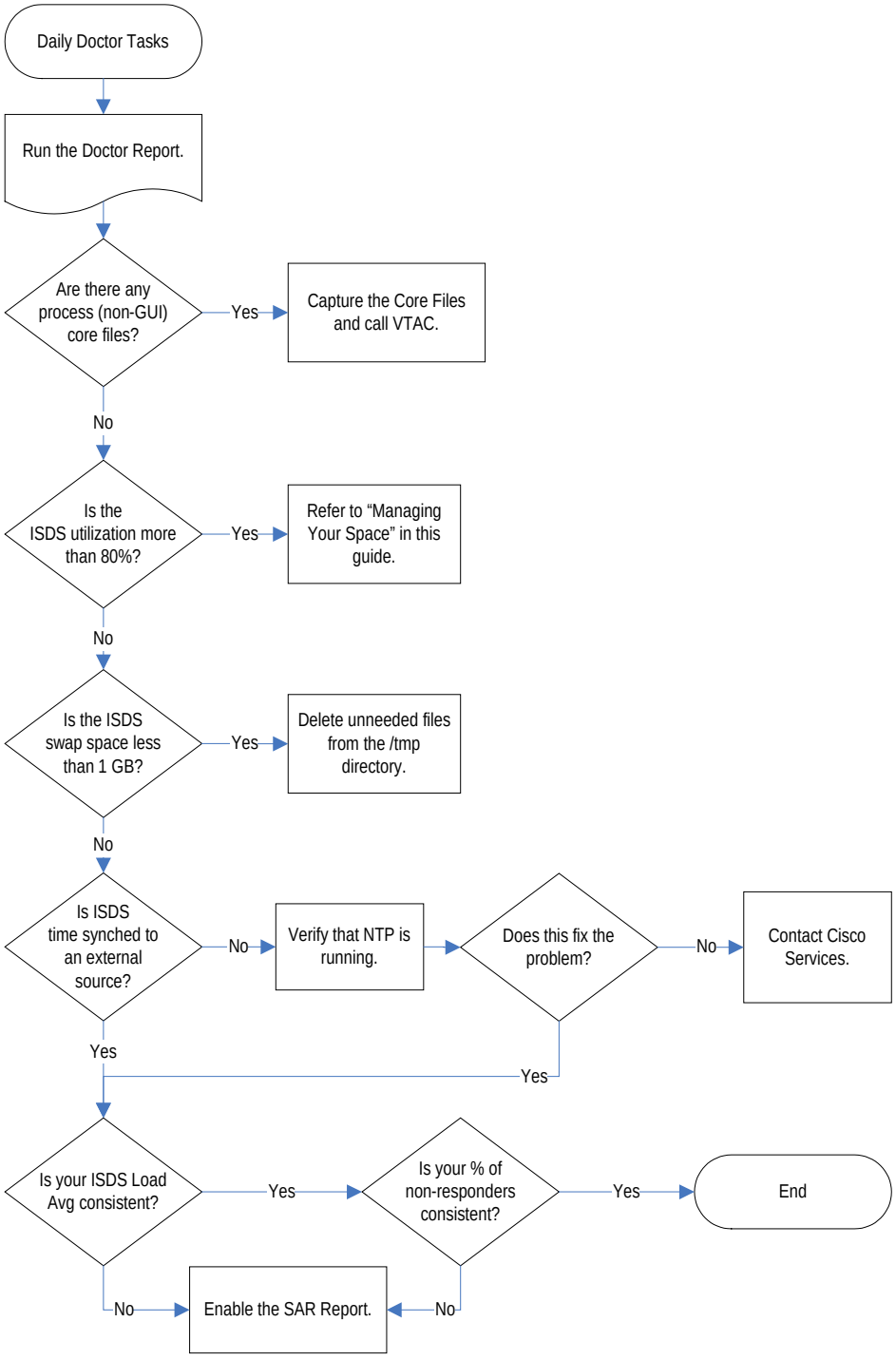
Objective	Tips	Passed?	Passed?
Average round-trip time for a 1-minute PCG ping is consistent.	The ping command is **ping -s [host_ip] 2000**. After this has run for a minute, press **Ctrl-C**. The ping will return packets lost and average round-trip time.	□ Yes □ No	□ Yes □ No
Average round-trip time for a 1-minute DHCT ping is consistent.		□ Yes □ No	□ Yes □ No
You can purchase, view, and cancel PPV events.		□ Yes □ No	□ Yes □ No


Other Twice Daily Tasks
Yes
Are the PCG ping times consistent?
No
Verify network connectivity.
Does this fix the problem?
No
Contact your network administrator.
Yes
Yes
Are the DHCT ping times consistent?
No
Verify network connectivity.
Does this fix the problem?
No
Yes
Yes
Can you purchase, view, and cancel PPV events?
No
Are all of the ppv processes running?
Yes
Contact Cisco Services.
Yes
No
No
Right-click and stop the process, then restart it.
Does this fix the problem?
End
Yes

Doctor Report Checks - Perform Once Daily

Date:_____**Check Time**:_____

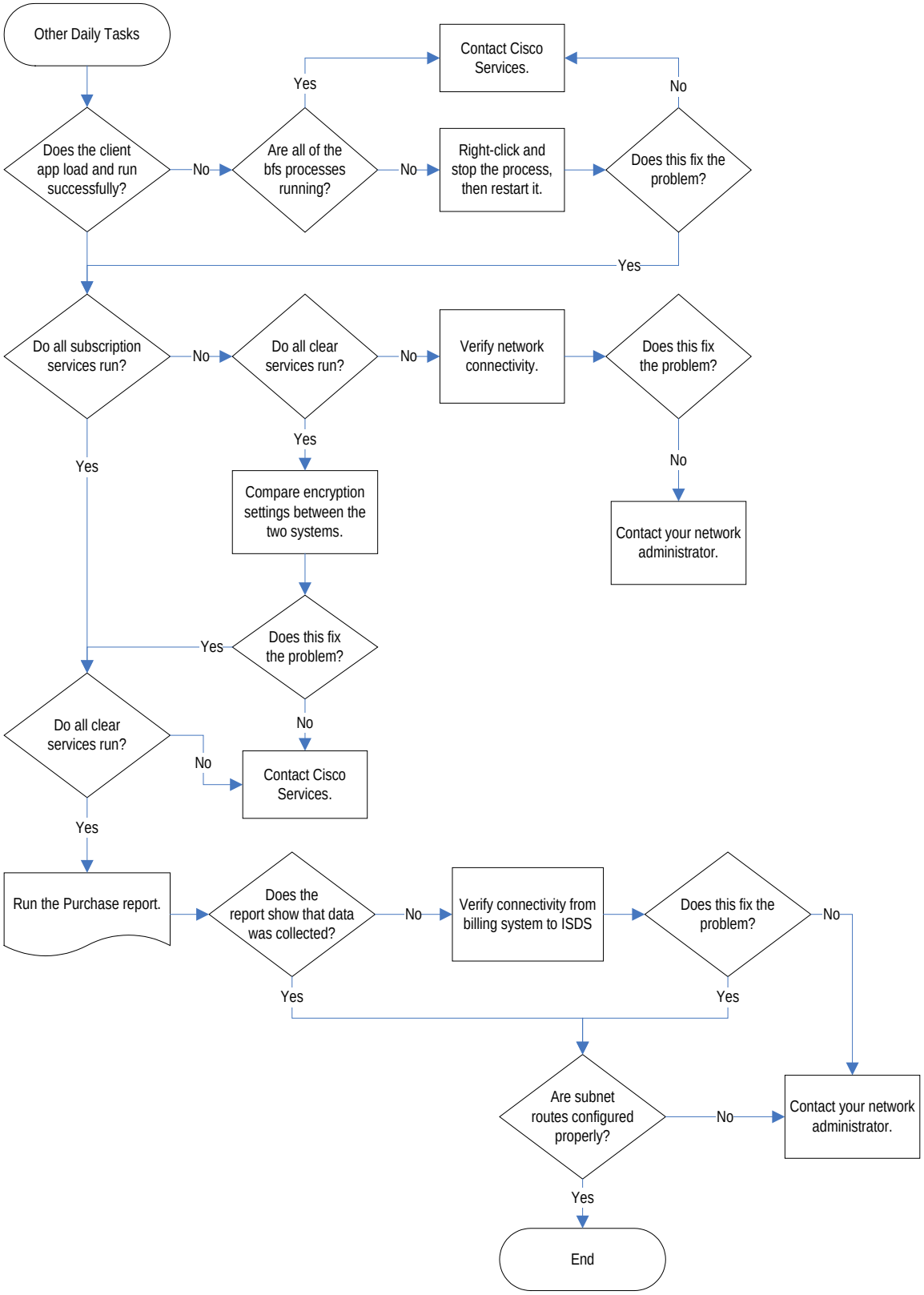
Objective	Tips	Passed?	
No process corefiles exist.	Capture all corefiles and deliver to VTAC, especially if they occur near the time of another problem.	☐ Yes	☐ No
Each ISDS volume utilizes less than 80 percent of its space.	See ***Managing Your Space*** (on page 7) for more information.	☐ Yes	☐ No
ISDS swap space is more than 1 GB.		☐ Yes	☐ No
ISDS time is synched to an external source.		☐ Yes	☐ No
The ISDS load average is consistent.	Compare to the previous day's load average.	☐ Yes	☐ No
The percentage of non-responders on the database report is consistent.	Compare to the previous day's percentage.	☐ Yes	☐ No


Daily Doctor Tasks
Run the Doctor Report.
Are there any process (non-GUI) core files?
Yes
Capture the Core Files and call VTAC.
No
Is the ISDS utilization more than 80%?
Yes
Refer to "Managing Your Space" in this guide.
No
Is the ISDS swap space less than 1 GB?
Yes
Delete unneeded files from the /tmp directory.
No
Is ISDS time synched to an external source?
No
Verify that NTP is running.
Does this fix the problem?
No
Contact Cisco Services.
Yes
Yes
Is your ISDS Load Avg consistent?
Yes
Is your % of non-responders consistent?
Yes
End
No
Enable the SAR Report.
No

Additional Checks - Perform Once Daily

Date:_____**Check Time**:_____

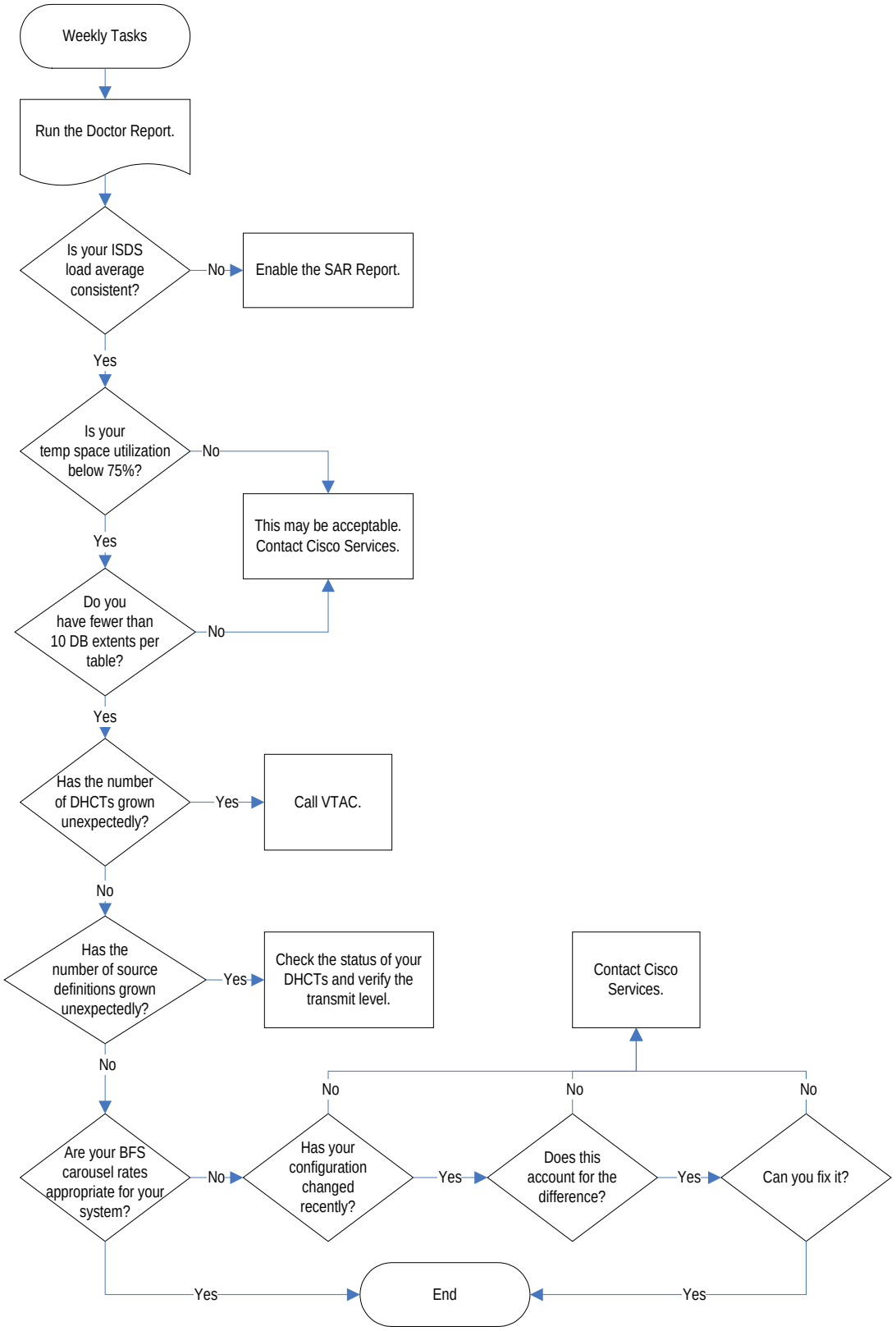
Objective	Tips	Passed?	
The client application loads and runs successfully.		☐ Yes	☐ No
All subscription services run.		☐ Yes	☐ No
All clear services run.		☐ Yes	☐ No
The Purchase Report indicates that information was collected.		☐ Yes	☐ No
All subnet routes are configured properly.		☐ Yes	☐ No


Other Daily Tasks
Does the client app load and run successfully?
No
Are all of the bfs processes running?
Yes
Contact Cisco Services.
No
Right-click and stop the process, then restart it.
No
Does this fix the problem?
No
Yes
Yes
Do all subscription services run?
No
Do all clear services run?
No
Verify network connectivity.
Does this fix the problem?
No
Contact your network administrator.
Yes
Yes
Compare encryption settings between the two systems.
Does this fix the problem?
Yes
No
Do all clear services run?
No
Contact Cisco Services.
Yes
Run the Purchase report.
Does the report show that data was collected?
No
Verify connectivity from billing system to ISDS
Does this fix the problem?
No
Yes
Yes
Are subnet routes configured properly?
No
Contact your network administrator.
Yes
End

Perform Weekly

Date:_____**Check Time**:_____

Objective	Tips	Passed?
Verify that the ISDS load average is consistent.	Compare to the previous week's check. (This field is called "DNCS Load Average" on the Doctor Report.)	☐ Yes ☐ No
Keep the tempspace utilization below 75%.	Warning: 75-84% utilized Error: 85% or greater These values will vary depending on how much memory you have allocated for tempspace.	☐ Yes ☐ No
Database table extents show fewer than 10 extents per table, depending on the size of the table and the frequency of use. (For example, HCT_PROFILE is used heavily and would be affected by excessive extents.)		☐ Yes ☐ No
Monitor the number of set-tops for growth.		☐ Yes ☐ No
Monitor number of source definitions for growth.		☐ Yes ☐ No
Make sure that the BFS carousel rates match the engineered values for your system. Refer to the Data Carousel Rate Settings in *Initial Installation and Upgrade Instructions for the ISDS* (part number 4028676).		☐ Yes ☐ No


Weekly Tasks
Run the Doctor Report.
Is your ISDS load average consistent?
No
Enable the SAR Report.
Yes
Is your temp space utilization below 75%?
No
This may be acceptable. Contact Cisco Services.
Yes
Do you have fewer than 10 DB extents per table?
No
Yes
Has the number of DHCTs grown unexpectedly?
Yes
Call VTAC.
No
Has the number of source definitions grown unexpectedly?
Yes
Check the status of your DHCTs and verify the transmit level.
Contact Cisco Services.
No
Are your BFS carousel rates appropriate for your system?
No
Has your configuration changed recently?
Yes
Does this account for the difference?
Yes
Can you fix it?
No
No
No
Yes
End
Yes

Other Checks

Date:_____**Check Time**:_____

Perform Every Two Weeks

Objective	Tips	Passed?
Run the EMM Deleter and delete all unneeded staging EMMs.	You determine which EMMs to delete, based on the age of the EMMs.	☐ Yes ☐ No

Perform Every Month, Every Three Months, or After Every System Upgrade

Objective	Tips	Passed?
Create a complete image of your system.		☐ Yes ☐ No

Perform After Spring and Fall Time Changes

Objective	Tips	Passed?
Check DST (Daylight Saving Time) settings to ensure all hubs and DHCTs are set correctly.	Doctor reports what DST settings are in place.	☐ Yes ☐ No

8

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.

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

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

October 2012 Printed in USA

Part Number 78-4030786 Rev C