Network Operating Software

8920 Network Trouble Patterning | Release 13.4

System Administration Guide

190-405-573R13.4
Issue 1
January 2012

Contents

A Reference Database Tables

About this document

Purpose

The book is written for both system administrators and O&M (Operations and Maintenance) personnel who work on Network Trouble Patterning (NTP) software once the application is installed on the NTP platform.

This book covers NTP-specific tasks only and is not intended to describe administration, operations, and maintenance tasks covered in vendor documents for the computer on which the NTP application runs (also see "List of documents" (p. xxvii) and "Prerequisites" (p. xxx)).

Audience

Responsibilities

Administration and O&M may be performed by the same individual, or the functions may be separate areas of responsibility.

- *System administration.* This book tells system administrators how to do such common tasks as start and stop NTP, update the reference data tables, add and delete NTP and BB-GUI users, set thresholding and alerting parameters, archive and retrieve surveillance data, and monitor error and other logs.
- *Operations and maintenance.* Appendix C, "Application Backup and Recovery" provides procedures to back up and recover the NTP application and the Oracle databases. O&M personnel may also refer to Chapter 2, "Start and Stop" , which includes procedures to stop and start NTP.

Documents

List of documents

The documents are as follows:

Document	Audience	Explains how to...
BB-GUI User's Guide 190-405-572R13.4	Network or revenue analysts	Use the browser-based graphical user interface (BB-GUI).

Document	Audience	Explains how to...
System Administration Guide 190-405-573R13.4	System administrator and O&M persons	Administer users and databases; perform application backup and recovery; start and stop the application.
Installation Guide 190-405-575R13.4	Installation personnel	Install NTP on a *Sun* machine.

About documents

- *Comments.* If you have comments or suggestions about the NTP documents, contact your NTP support organization.
- *Ordering.* Follow your company's procedures to order additional copies of documents.
- *Reproduction.* You can reproduce these documents. Please do not release copies outside your company.
- *Media.* Documents are available in .pdf on CD-ROM. Also, the BB-GUI offers all documents in .pdf format and in HTML format. You can print from .pdf.

Software Release Notes and Third Party Software License Information

Location of Release Notes

For a comprehensive listing of new features and enhancements made to the NTP software for the most current generic, see the NTP Release Notes.

To access the Release Notes, direct your Web browser to the following URL:

`http://<host_and_domain>:4618/info/release_notes.pdf`

where:

`<host_and_domain>` is the path you normally use to access the NTP launch page. For example:

- a machine name, such as hpn42.cb.lucent.com
- an IP address, such as 135.7.59.47.

`4618` is the apache port number.

Reference: To change the default port number, see “How to Change Default Port Number for Apache, Apache with SSL, and OpenLDAP” (p. 9-4) .

Third Party Software License Information

The NTP software makes use of various third party software packages. A complete listing of those packages and their associated copyright and/or license information is available in this document, immediately following the document Table of Contents, and on the BB-GUI.

Access this information on the BB-GUI by:

1. Clicking on the Additional Help Topics icon, found in the upper-right corner of the Launch Page,
2. Selecting "Copyright" from the drop down menu,
3. Clicking on the "Third Party Software" link at the bottom of the Copyright page.

Customer Support

Obtaining support for NTP

You can obtain customer support for the NTP product in several ways:

- Call 1-866-LUCENT8 (1-866-582-3688) and select prompt 5.
- If you have registered with the Customer or BusinessPartner Center (i.e., you have a CARES login), you can create a request for a priority 3 or 4 AR online via the Customer Assistance Request Entry System (CARES) web site at https://cares.support.lucent.com.
- Access the Alcatel-Lucent Customer Support web site at http://www.lucent.com/support/ to register for online customer support.

Prerequisites

System administration

To administer the NTP host, system administrators need prior experience in routine tasks such as (but not limited to) the following:

- Common file manipulation for your operating system, such as editing (through **`vi`** or another ASCII text editor), moving and removing files
- Routine system and user administration, such as adding, deleting, and administering users; using *cron* and other operating system utilities; shutting down and restarting applications and utilities.

Operations and maintenance

Before performing maintenance on the NTP host, you need experience in routine tasks such as (but not limited to) the following:

- Halting and booting the application host machine
- Recovering file systems to a disk from its mirror
- Recovering individual files from a *tar* -compatible backup tape.

We assume the following:

- Maintenance on the computer platform on which the NTP software runs is the customer's responsibility, either through a maintenance contract or through other means. Procedures for operation and maintenance of the platform hardware and software are NOT described in the NTP documents. Instead, see the vendor documents for your system.
- Generally the NTP host hardware and software is installed by the NTP support organization. Self-installation is available as a purchasable feature. Customers utilizing this feature can refer to the *Installation Guide* (190-405-575R12.1).
- The NTP administrator should have access to:
  - Reference documents for the NTP host and *Oracle* database
  - All NTP user manuals.

Format, Typography, and Conventions

Shell users

Keyboard

Commands you type or enter at the keyboard appear in bold print. For example, the instruction to "enter **`cd $SNASDIR`** " means to enter the exact characters in bold-faced print. Variables are shown in *italic* print regardless of where they appear.

Example: Enter **`sui find so=acode delim=' ";" ' > /tmp/acode`** where `/tmp/acode` is a temporary file.

References to keyboard keys appear in bold print. For example, **Delete** means the Delete key, **Escape** means the Escape key, and so forth.

The word "enter" means to type input and then press **Return** . The word "type" means to type input without pressing **Return** .

In special cases, further information is provided for keys. For example, the instruction to press **Control d** means to press and hold the **Control** key while simultaneously pressing the letter **d** key.

Prompts and output

System prompts are shown in the standard print for the documents. System output and messages are shown in constant width ("typewriter") print.

Environment variables

Throughout the user documentation, environment variables are used in pathnames and command lines. This is because the application home may be installed at a location different from the default.

- In almost all cases where input is required, you can enter either the actual path or the appropriate environment variable.
- Examples of output throughout the user documentation assume that the application home is */lucent/ntp/snas* .

How to comment

To comment on this document, go to the Online Comment Form (http://infodoc.alcatel-lucent.com/comments/) or e-mail your comments to the Comments Hotline (comments@alcatel-lucent.com).

1 System Description

Overview

Purpose

This chapter provides a high-level view of the Network Trouble Patterning software system.

Topics covered include:

- “Users” (p. 1-3)
- “Hardware and Software, and Connectivity” (p. 1-6)
- “Files and Databases” (p. 1-31)
- “Administrative Tools and Routine Tasks” (p. 1-38)

Contents

Users

Introduction

Logins and permissions

The NTP administrator assigns logins to users, which they use to access NTP. This table shows the administrator's responsibility.

Login, ID, or permission	Purpose	Comments
root login	The operating system **root** login on the NTP host.	None. These logins are configured when NTP is installed.
ntp login	The NTP administrator login on the NTP host. Can execute NTP commands that other administrative logins cannot (including **ntpstart** and **ntpstop**).	
NTP administrative logins (typically a different login for each administrator)	Allows administrative users to manage NTP with: • System tools (such as SAM), and shell/ksh commands such as **vi** • NTP administrative commands, such as **linkmon** • The NTP SUI (shell user interface)	User permissions and restrictions depend on standard user administration for the operating system, including shell assignment. Users may also be restricted by command group.
NTP user logins (typically a different login for each user)	Required for all users to access NTP.	

Login, ID, or permission	Purpose	Comments
BB-GUI IDs	Required to access the BB-GUI and execute its pages.	"Add a BB-GUI user" (p. 6-54). Select the checkbox in the Permission field to give a user administration permission.
BB-GUI web user administration permission	Required for web administrators to: • Assign BB-GUI user IDs • Set default BB-GUI user preferences • Create, modify, and delete preferences for all BB-GUI users • Create, modify, and delete global saved searches and table layouts.	

Permission for other systems

An NTP administrative login does NOT enable a user to administer OTHER systems or networks which NTP may be integrated, such as:

- TCP/IP networks
- Sources that forward CIMs to NTP
- Entities from which NTP receives data.

User Interfaces

Description

This table describes the interfaces to NTP. NTP administrators require the SUI and shell, and may use the GUI. Analysts require only the GUI, but may be given access to other interfaces.

Interface	Users	Description	Method
BB-GUI	Network and revenue analysts	Browser-based graphical user interface accessed via a web browser	Point and click
SUI	NTP administrators	Shell user interface used to execute a special set of NTP commands, which are prefixed with **`sui`**. See Appendix B, "SUI Commands".	Keyboard in operating system shell
Shell		Used for running operating system commands and NTP commands that do not require the **`sui`** prefix.	Keyboard in operating system shell

Hardware and Software, and Connectivity

Introduction

Purpose

This section discusses the hardware NTP runs on, and two levels of software running on the hardware, as follows:

- *Operating system software*. Runs the shell interface.
- *Application software*. Runs NTP. You can run this only if the operating system software is running.

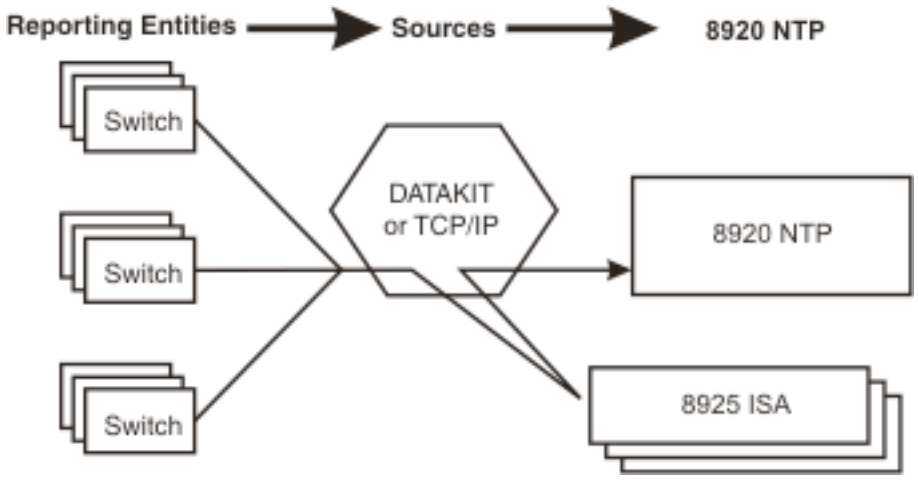
It also includes a section on TCP/IP connectivity.

Important! Not mentioned here are several third-party software applications included with NTP software, such as Oracle database software.

Configuration illustration

This illustration shows that NTP software runs on the NTP host, regardless of where output is displayed or what interface is used.

Important! Client software is necessary to run the BB-GUI. See "Hardware and Software" (p. 1-7).



Hardware and Software

Overview

The NTP software runs on the following hardware and operating systems:

Element	Hardware	Software
NTP host computer	*Sun*	*Solaris* 10 operating system
PCs for the BB-GUI Note that other configurations may be supported. Contact your NTP support organization.	The hardware configuration for a NTP solution is highly dependent upon the data rate, data elements, the number of users and the long-term data storage requirements. • PCs — Minimum Pentium 1GHz processor, 1 GB of memory, 4-GB hard disk with 1 GB free space, 32-MB or 64-MB 32-bit video card, PC display set to "high" or "true" colors, and SVGA monitor set to 1024x768 resolution. In addition, Pattern Painter requires 5MB of space in the user's home directory on their PC (for example, *C:/Documents and Settings/<userid>/Local Settings/Application Data*) for every 10,000 records. This is up to 15MB of space for the maximum of 30,000 records.	Operating system: • *Windows XP Pro SP2* with latest cumulative patches • *Windows 7* with latest cumulative patches. Browsers: • *Microsoft* Internet Explorer version 7 and 8 and Mozilla Firefox version 3.6.X Client software: • Web GUI CLIENT software (one CD)
Printers	Configuration of printers to print from BB-GUI clients is the customer's responsibility and is not covered in this book.	

Note: NTP, from release 13, does not support the HP platform as well as *HP-UX* operating system, but might support upon customer request.

Customer-installed client software

BB-GUI client software

Users running the BB-GUI must have BB-GUI client software installed on their PCs. The NTP support organization installs this software during initial system installation. However, thereafter, the NTP administrator is responsible for installing it when new BB-GUI users are added.

Important! If user will try to access any BB-GUI page from a machine without the Java plug-in installed, the browser will automatically be redirected to a client installation page. The Java JRE is not delivered with the BB-GUI client software. Consult your internal IT department for information on how to obtain and install the Java JRE, or visit the official Sun Java website.

The current officially supported versions of Java JRE are:

- Java SE Runtime Environment (JRE) 6 update 20

Pattern Painter software

Pattern Painter runs in association with the BB-GUI to display graphical depictions of data. Users running Pattern Painter must have Pattern Painter client software installed on their PCs. The NTP support organization installs this software during initial system installation. However, thereafter, the NTP administrator is responsible for installing it when new Pattern Painter users are added. The Pattern Painter software includes the following components:

- NTP Advizor executable
- Pattern Painter components.

Hint: See "Install and Uninstall Client Software for the BB-GUI" (p. 6-60).

Disabling pop-up blocker warnings for Pattern Painter sortware

By default, your Internet browser blocks pop-up windows on web sites and displays a warning message. Disable pop-up blocking to allow Pattern Painter to display graphical depictions of data in new windows.

To disable pop-up blocker warnings, do the following steps:

1. Open Internet Explorer
2. On the **Tools** menu, click Internet Options
3. On the **Advanced** tab, under **Security**, check the following option: **"Allow active content to run in files on My Computer"**

Other customer-installed software

The Adobe Reader software is recommended to read user documentation files provided in pdf (Portable Document Format), accessible from the BB-GUI. This software is available at no cost from the Adobe System, Inc. website (http://www.adobe.com).

TCP/IP Connectivity

Purpose

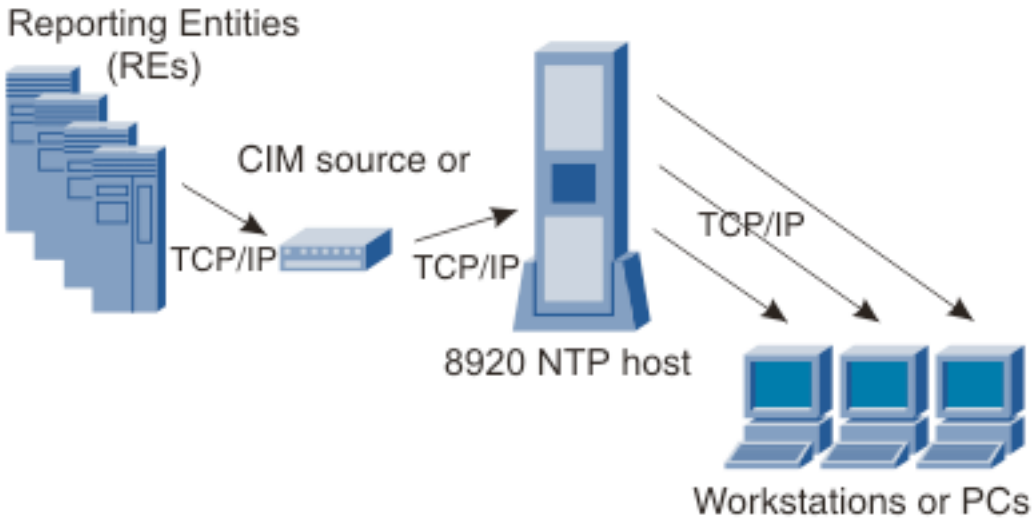
Various hardware elements in NTP systems are connected by TCP/IP.

Important! *Datakit* is not directly supported by NTP. For some installations, *Datakit*-to-TCP/IP conversion may be required. Conversion is typically done through customer-provided hardware and software that allows mapping of *Datakit* dialstrings to TCP/IP ports and addresses. Consult with your NTP support organization.

User interface connections

This illustration shows where TCP/IP connections are used.

- Reporting entities send CIM (call information message) data to a collector, which is known in NTP as a "source," over TCP/IP links.
- The source forwards the CIMs to NTP over TCP/IP links. The CIMs may be in a data stream or in file-based format.



Other Interfaces and Features

Many Optional Features

NTP offers core functionality that can be enhanced with optional features. Some of these features must be purchased (e.g., *Sonus* Softswitch Support). Other features do not need to be purchased individually, but may be elected or rejected based on each customer's particular needs (e.g., TN Grouping features). Only Alcatel-Lucent personnel may enable and disable features.

Reference

See the *Installation Guide* , Chapter 3, "Installation", for more information about feature optioning, and Appendix A, “Core and Optional Features”, for more information about the core and optional features pertaining to each solution of the NTP product.

System Administrators may find it useful to run the **`listopt`** command, which displays a list of all features and their status (enabled or disabled), and refer to the output when using the information in this manual.

Sample output of the **`listopt`** command is shown here:

```
MDIISS7           6370 - MDII Operator Services over SS7    disabled

MDIISS7           6370 - MDII Operator Services over SS7    disabled

MESSAGE_BROADCAST 6374 - BBGUI Message Broadcast            enabled

MINT              6224 - 5ESS MINT Support                  disabled

MT20_CONV         6288 - Alcatel MT20 Converter             disabled

MULTISIG          6059 - Multiple Signaling Network Supp    enabled

NAVISID           6385 - Navis ID Integration Support       disabled

NETSEG            6001 - Network Segments                   enabled

OSPSCONV          6011 - 5ESS OSPS OTR Support              disabled

OTRSUMM           6178 - OTR Summary Table                  disabled
```

8925 Integrated Service Assurance (ISA) Platform

The 8925 Integrated Service Assurance and Network Fault Management software platform integrates the family of network operating software products, providing a common view across the network. ISA allows the user to utilize data to monitor the performance of their voice services, data network, signalling network and more from one central location.

NTP offers the ISA interface as a purchasable feature. With this feature, NTP provides alerting data, reference data, and drilldown information to ISA. Once enabled on the NTP side, NTP receives requests from ISA, verifies the IP address, and sends data to the ISA every 5 minutes.

Secure Socket Layer Protocol

The Secure Socket Layer protocol, developed by *Netscape* , is used for authenticating and encrypting data passed over the web.

NTP offers the SSL protocol as a purchasable feature. The feature configures the web server and the CORBA server on the NTP host to provide SSL encrypted communication between the servers and a browser for the http protocol.

With this feature, the browser-based GUI can be accessed in one of the following modes:

- http or https (This is the default configuration. The user selects whether or not to access a page using SSL encrypted communication.)
- https only (Communication is always encrypted.)
- http only (Communication is never encrypted.)

  Important! Customers using custom network configurations (e.g, gatekeeper ports used with SSL) must specify ports less than 32768.

Reference: See "How to Change Default Port Number for Apache, Apache with SSL, and OpenLDAP" (p. 9-4) for information on the required default port numbers.

Data Flow

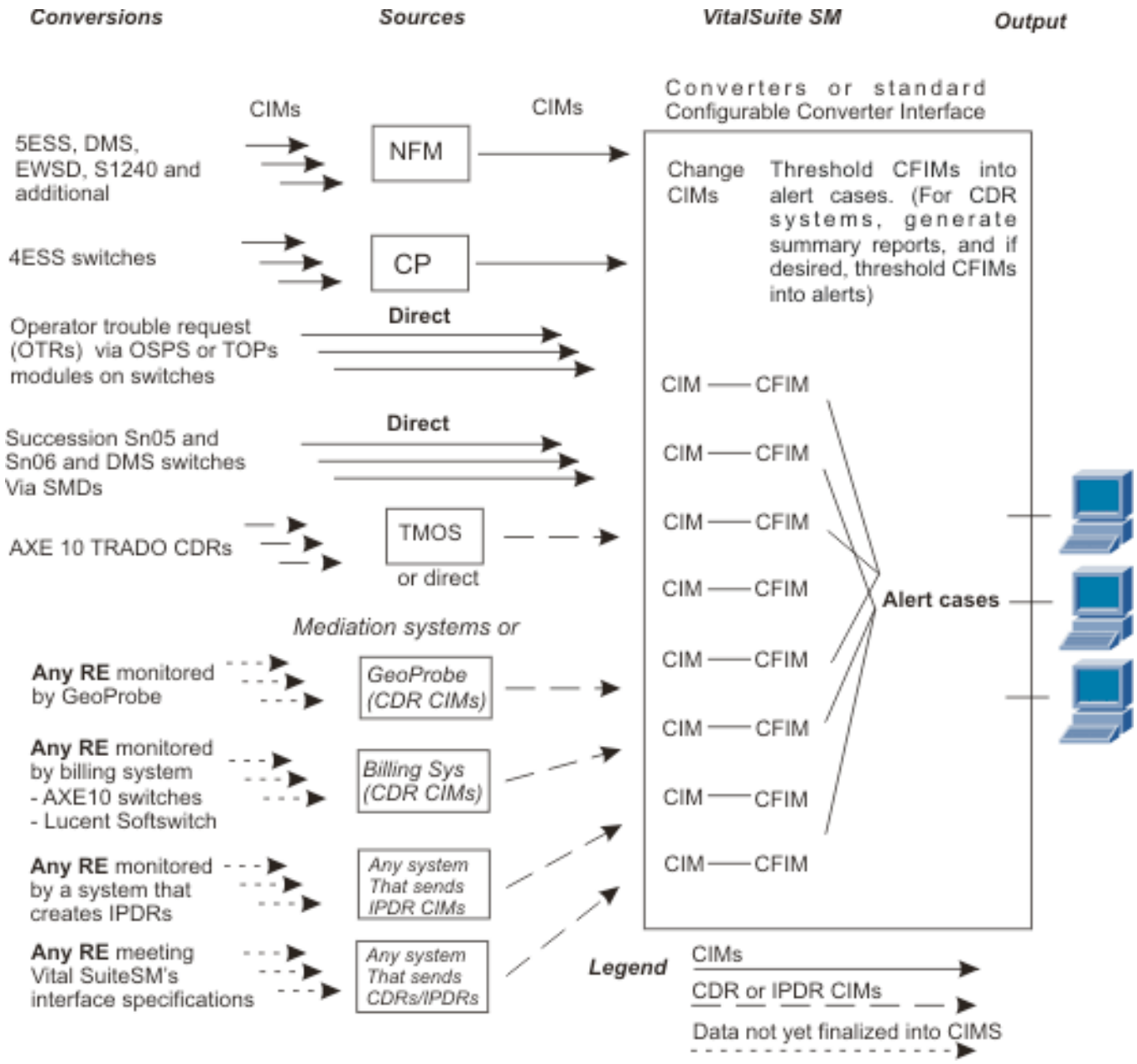
Overview

Purpose

Knowing where output comes from is important for network troubleshooting or analysis.

Data flow illustration

This illustration shows how surveillance data flows to output.



Data flow terms

Terms used in the data illustration are:

- *Reporting entities (REs)*. An element in your network that reports to NTP. Each customer has only some types of REs.
- *Sources*. Gather CIMs from REs and forward them to NTP. See "Sources" (p. 1-17).
- *CIM*. Call information message. See "CIMs" (p. 1-16).
- *CFIM*. Common format call information message. NTP takes CIMs in various formats and puts them into a standard format.
- *Alert case*. If a problem's CFIM count is above threshold, those CIMs are tallied into an alert case.
- *Output*. You see alert cases, CFIMs, CIMs (though some CDR CIMs may be discarded), summary reports, and other outputs.

Data flow stage table

This table explains the flow of data to and through NTP. See other information in this section for a more complete understanding.

Stage	Traditional CIMs	CDR CIMs
1	*REs send CIMs to a source*. REs (usually switches) create traditional CIMs and send them to an EMS source (or directly to NTP)	*REs send data to a source*. REs send data to a mediation system source, so the source can create the CDR CIMs (or the RE may send CDRs directly)
2	*Source sends CIMs*. The source forwards CIMs to NTP.	
3	*Convert CIMs to CFIMs*. NTP translates CIMs to CFIMs (common format information messages), making them easier for you to read and analyze.	
4	*Summarize data*. NTP summarizes CFIMs into summary tables used for summary reports.	
5	*Count*. NTP groups CFIMs into sets and counts the problems in each set.	
6	*Threshold*. If the count in a set crosses a threshold, the problem is handled as an alert case. Then, periodically: • *New*. If a count crosses threshold for the first time, a new alert case is added to Alert cases page. • *Existing*. If a count crosses threshold for an alert case already on Alert cases page, the alert case's tallies (such as the Count field) are incremented. *Hint: See* "Thresholding overview" (p. 1-18).	

Stage	Traditional CIMs	CDR CIMs
6	*Close alert cases*. An alert case automatically closes, and drops off of Alert cases page output, if its CFIM count has been below threshold for 2 hours (if its total CFIM count is less than 50) or 4 hours (if its total CFIM count is more than 50). • These are default times—your system administrator can change them. • Below-threshold intervals are counted in the Cai fields. • Users can manually close alert cases.	
7	*Purge data*. Active alert cases stay on Alert cases page potentially forever. But CIMs, CFIMs, and closed alert cases are eventually purged. How long they are retained depends on your traffic and your data storage capacity. Ten days is a typical minimum retention period.	

Contents

CIMs

Description

Traditional systems process mostly CIMs (call information messages). Traditional CIMs:

- Report lost calls (almost always)
- Are generated by the RE and typically forwarded to an EMS (element management system), which forwards them to NTP. They may instead be forwarded directly to NTP from a module associated with an RE.

CDR systems process CIMs related to call completions, including CDRs (call detail records) and IPDRs (internet protocol detail records). Collectively these are referred to as CDRs. CDR CIMs:

- Report session data, such as billing information, typically NOT lost calls.

Please note that some CDRs may represent lost calls. For example *GeoProbe* collects CDR CIMs that are mostly for lost calls.

- Are typically generated by a mediation system, but may be forwarded directly to NTP from a module associated with an RE.

Sources

Description

The ultimate source for CIMs is reporting entities REs (see "CIMs" (p. 1-16)). What NTP calls a "source" is really an element that collects or forwards data from REs to NTP. (See "Data flow illustration" (p. 1-13).) Even a direct interface can be a "source" for NTP administrative purposes. Each source is defined in the NTP reference database, and physical and logical links must be established between the source and NTP. This table (source) summarizes source types.

Hint: See Chapter 5, "CIM Source Administration"

Source type	Description	Retype
Mediation system	Typically forward CDR CIMs (success or usage messages. *Example:* • Billing mediation systems that reformat CDRs, such as *CSG Data Mediation* (formerly BILLDATS data manager) • IP network monitoring systems that create IPDRs	*Many* — CFIMs from one mediation system can have different Retypes (a different Retype for each entity type the system monitors). The CFIM's Source field (NOT its Retype field) hints at which CIM-to-CFIM converter was used.
EMS (element management system)	Typically forward traditional CIMs (typically, failure messages). *Example:* • Lucent NFM (OneVision Network Fault Management) system or NOC1 • *Ericsson TMOS* (Telecommunications Management and Operations Support) system	*Typically one per source* — Typically, CFIMs from one EMS all have the same Retype (such as 5ESS). The CFIM's Retype field (AND its Source field) hints at which CIM-to-CFIM converter was used.
Direct interface	An interface is established between NTP and the RE (or associated RE module). *Example:* • *Nortel SDM* (Supernode Data Manager) • OTR *DMS TOPS* or *5ESS* OSPS modules	*Retype — one per source*. Typically the RE cannot be identified UNLESS it is associated with a source. Typically one source is administered per RE.
Note that theoretically, you may see two CFIMs with the same RE, but the Source field on one holds an EMS (such as an NFM), and on the other holds a mediation system (such as a *GeoProbe*).		

Thresholds

Thresholding overview

NTP thresholds on a set of CFIM fields known as an FQ (fundamental quantity). You can threshold on any FQ set up for you by Alcatel-Lucent consultants.

The default FQ is:

- FDC
- RE or DE
- LSP (Load set period) The week is divided into LSPs (traditionally, 48 LSPs).
  For each FQ, there are two sets of thresholds for two types of intervals:
  - *5-minute*. Detects bursty problems.
  - *Hourly*. Detects chronic problems.

  Example: With 400 FDCs, 20 REs, 200 DEs, two intervals (5-minute and hourly), and 48 LSPs, you could have up to 8,448,000 thresholds.

  Important!

  - Thresholds are automatically created during a 2-week "soak". After that, they are automatically adjusted at every LSP, so that routine and seasonal changes to calling patterns are not misinterpreted as problems. This is adjustable. The default is 10 iterations of each LSP, so it would take 2 weeks to soak the weekdays and 5 weeks for the weekends.
  - The system administrator can assign thresholds manually. For example, for an FDC indicating 911 problems, you may want a manual threshold of 1.

Hint: See Chapter 8, “Threshold Administration”.

Conversions

Which entities can be REs

Virtually any type of network element can be an RE, depending on conversion. A conversion translates CIMs to CFIMs. By "conversion" we mean not just the software module used (such as the Configurable Converter), but the set of tables and fields the NTP support organization or the NTP system administrator populates to convert a specific type of CIMs to CFIMs.

For many interfaces, the standard NTP interface (Configurable Converter) can be used. For more information, see "Recognize a CFIM's conversion by Retype on CFIM" (p. 4-12).

CIM types

You may need to ask the administrator of an RE to ensure the RE is creating the CIMs you need. This table lists CIMs by conversion (retype field in CFIM output). For more information on conversions, see the *BB-GUI User's Guide*.

Conversion (CFIM retype)	CIMs
1aess	Lucent 1A ESS messages: • TN08 • CCS7 RTN. CCS7 Return messages. • CCS7 UPC. CCS7 Unknown Point Codes. • SCP ALERT.
4ess	Lucent 4ESS traps: • FHC, IMA. Final Handling Code of IMA (Ineffective Machine Attempt). • FHC, INA. Final Handling Code of INA (Ineffective Network Attempt).
5ess	Lucent 5ESS MDII. Machine Detected Interoffice Irregularity.
5e assert	Lucent 5ESS Assert messages: • RTA DCF • MANUAL
osps (5ESS)	OTRs from an OSPS (Operator Services Position System) module on a 5ESS. Some OTRs also contain LNP data.

Conversion (CFIM retype)	CIMs
tops (DMS)	From a *DMS TOPS* (Traffic Operator Position Systems) module on a *DMS. DMS* logs (xxx means three digits) include: • SNAC100 (operator trouble reports). • TOPSxxx. Reports on LNP, validation (credit card, coin call, etc.), and operator assisted calls.
Autoplex MSC	AUTOPLEX MSC ROP (Read Only Port) messages: • MDII. Machine Detected Interoffice Irregularity. Reports interoffice irregularities that occur on trunks during a call setup • AUTH FAILURE. Authentication failure. This can be multiple reasons. Of particular interest for wireless providers is an increase in the number of these messages, which suggests there is a cell border problem. • CELL CP FAILURE. Cell call processing failure. This can result from 29 unique reasons (for which we assign 29 different FDCs), such as radio failures, encoder failures, vocoder mismatch, T-1 problems, TDM bus problems, glare (a mobile tried to originate a call when it was still marked as busy), and failed hand-offs. • REPT CELL HEH 2. Cell hardware error handler. This message can be generated for many hardware errors and information relating to specific cell site. NTP will independently threshold and alert for each of the unique reasons. Available only with Autoplex HEH Support feature. • REPT EVDO RNC CP FAIL. This message can result from 35 different failures (for which we assign 35 different FDCs), such as session setup failures or abnormal session terminations, idle or active hand-off failures, security failures, problems on the A10 (Bearer Path Interface)/A11 (Signaling Interface) data and control paths between the RNC (Radio Network Controller) and the PDSN (Packet Data Serving Node), problems with the A12 (Signaling Interface) control path to the AAA (Authentication server), problems with UATI (Universal Access Terminal Identifier) assignment, error conditions on the BTS (Base Transceiver Station) or the PDSN. To interpret AUTOPLEX CIMs, see the *AUTOPLEX Output Messages Manual*.

Conversion (CFIM retype)	CIMs
Autoplex MSC (follow-up)	AUTOPLEX MSC ROP (Read Only Port) messages: • IMCELL CP FAILURE. This message is similar to the CELL CP FAILURE except the cell reporting the problem does not belong to the MSC that created the message. When populating the CFIM, NTP will set the de field to "remote-" plus the cell identified in the message. • DCS CP FAILURE. Digital cellular switch call processing failure. This message reports call processing time-outs at the executive cellular processor (ECP) while waiting for a tone or announcement acknowledgment from the DCS. • GENERAL SYSTEM CP FAILURE. General systems call processing failure. This message can be generated for 12 reasons (for which we assign 12 different FDCs), such as no inter-MSC response, no VCA response, or database failure. • SCP DATABASE FAILURE. Failed SCP database queries. • DCS FAILURE. Failure at the DCS. The failure could be for a voice or data call. To interpret AUTOPLEX CIMs, see the *AUTOPLEX Output Messages Manual*.
dms	*DMS* logs for *DMS* 100, 200, 250, and 500. (xxx means three digits) • C7UPxxx. CCS7 User Part messages. • LINExxx. In-band call setup failures on an incoming line. • TRKxxx. Trunk messages about in-band call setup failures. • TCAPxxx. Transaction Capabilities Application Part - database query problems to an SCP. • LNPxxx. Local number portability logs for number portability routing failures. • AUDTxxx. Messages on incorrect trunk state and calls forced down by the release of a trunk. • E911xxx. Logs indicating problems with the delivery of emergency phone service.

Conversion (CFIM retype)	CIMs
dms-mtx	*Nortel DMS* MTX (Mobile Switching Exchange) MSC (Mobile Switching Center), for TDMA and CDMA (Code Division Multiple Access) mobile technology. The same *Nortel DMS* logs listed above, MINUS LINExxx, PLUS the following: • CELLxxx. Information about cellular systems and calls. (CELL1XX are for failed cell calls. CELL2XX are for testing cell calls. CELL3XX are for manual cell calls). • CLFLxxx. Call failures or events involving mobile units. • DROPxxx. Dropped cellular calls. • NPxxx. Number portability (requires that Number Portability Log feature be enabled).
nrtl-gsm	*Nortel DMS* MSC (Mobile Switching Center) logs, for GSM (Global System for Mobile Communications) technology. The same *Nortel DMS* logs listed above, MINUS LINExxx, and LNPxxx PLUS the following: • GBCSxxx, GSM Base Station Controller. • GINxxx, Intelligent Network. • GMSCxxx, Mobile Switching Center. • GBSSxx, Base Station Subsystem.
ewsd	Siemens *EWSD* trapped output masks: • 03832, trapped machine interoffice irregularity status (non-toll interoffice failure alarm levels). • 03833, trapped machine interoffice irregularity status (non-toll interoffice failures). • 02047, irregularity trap (for equal access toll call alarm levels). • 04393, irregularity trap (for equal access toll calls).
succ	*DMS* Logs. *Nortel Succession*, same as dms, but enhanced to include ATM data. Nortel Succession SN09 Support - backward compatibility and NTP software support of the C7UP, TRK, and TCAP log classes.
GeoProbe	*Geoprobe* CDRs. Call detail records (mostly about SS7 problems) from any switch monitored by a GeoProbe mediation system.
axe10	*AXE* TRADO messages. *Ericsson AXE* 10 switches, not from *CSG Data Mediation* (formerly BILLDATS data manager).
softsw	CDRs. Call detail records from a Lucent 3.1 Softswitch.

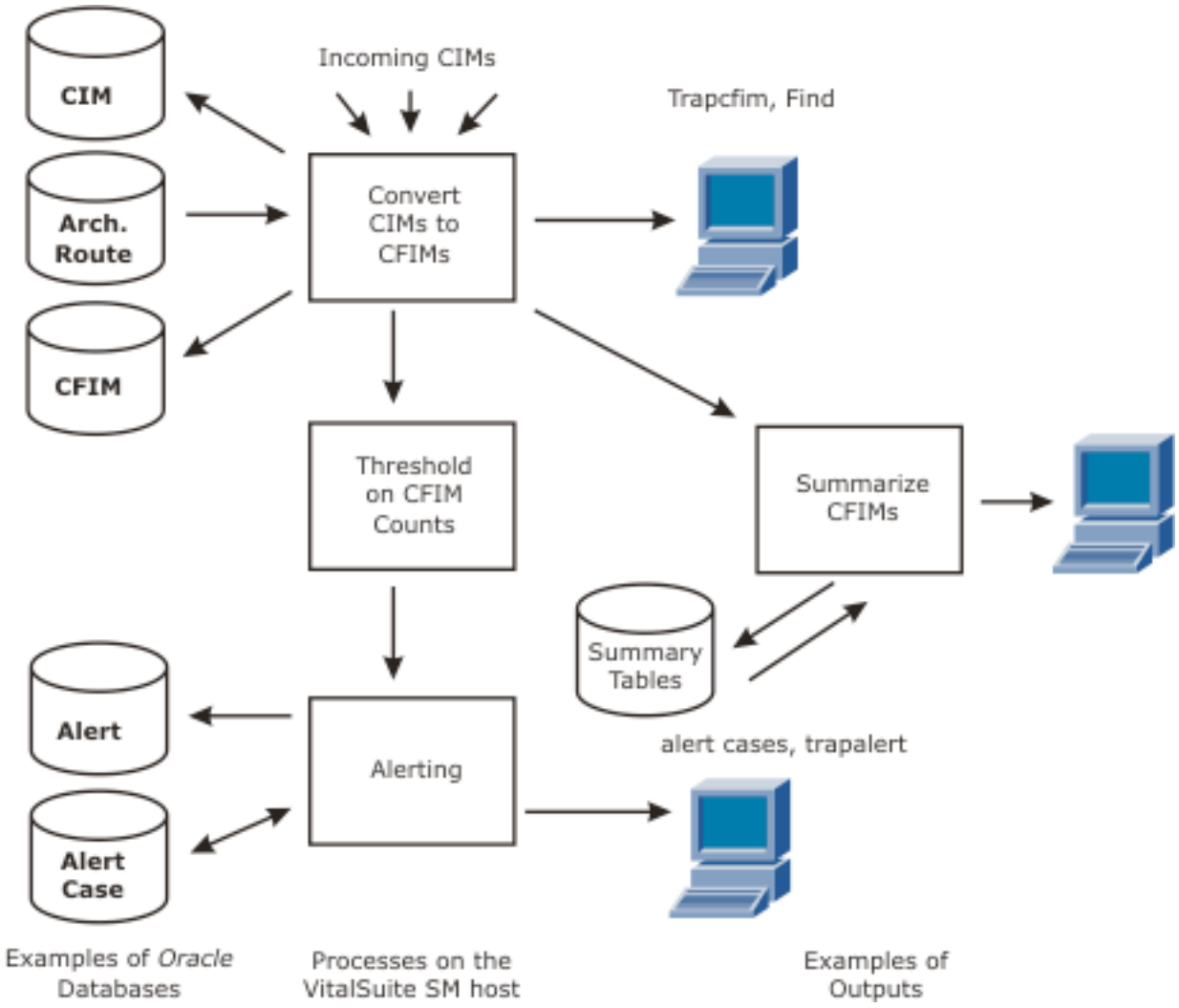
Conversion (CFIM retype)	CIMs
ip	IPDR (CDRs). Call detail records from a Lucent 3.1 Softswitch.
ccc (consultant added CDR conversion)	CDRs. Probably CDRs from a mediation system.
S1240	*Alcatel* S1240 Route Message Types: • 0121 Observation Call Sampling • 4330 Routing Administration
Sonus	CDRs. Stop and Attempt records.
Plexus	CDRs.
PCMD	PCMD (Per-Call Measurement Data) messages (applies only to Autoplex)
Alcatel 5020	CDRs generated by Alcatel 5020 Spatial Atrium Softswitch
Alcatel MT20	Call types: • 162 (incoming call) • 163 (outgoing call)
GTD-5	Syndrome 2.xxx and 3.xxx messages
GPRS	CDRs for General Packet Radio Service (GPRS) (based on 3GPP standard 32.015)
Ericsson GSM	CDRs for *Ericsson* Global System for Mobile Communications (GSM)
CCF	CDRs obtained from the Charging Collection Function (CCF) in an IP Multimedia Subsystem (IMS) core network (CDRs layout based on 3GPP TS 32.225 standard)

Conversion (CFIM retype)	CIMs
imsccf	CDRs obtained from the IMS core network. The received data cover the following components of the IMS core network: • Proxy Call Session Control Function (P-CSCF), • Serving Call Session Control Function (S-CSCF), • Interrogating Call Session Control Function (I-CSCF), • Breakout Gateway Control Function (BGCF), • Media Gateway Control Function (MGCF), • Media Gateways (MGs), • SS7 Signaling Links, • SS7, CAS, and BICC Trunk Groups and Channel Groups, • SIP Trunk Groups, • Border Element Gateway Pairs.
SIP log (Session Initiation Protocol)	Reports generated by S-CSCF (Serving Call Session Control Function) in an IMS core network: *SIP 4xx* - Client error - the request contains invalid syntax or cannot be fulfilled by this server *SIP 5xx* - Server error - the server failed to fulfill an apparently valid request
SDHLR OM	Output Message logs collected from the Lucent's Flexent SDHLR (Super-Distributed Home Location Register) via OMC-H (Operation and Maintenance Center)
FS3000	CDRs generated by BroadWorks® Broadsoft® FS3000 Feature Server Release 13.0. The CDRs are processed, stored and used for thresholding and alerting. The CDRs can indicate the following types of call failure problems: • Unallocated numbers, • Routing failure such as inability to request a route or unable to obtain a route, • User busy conditions, • Terminated calls or sessions rejected, • Destination out of order failures, • Temporary failures, • Manually terminated calls, • Calls terminated due to protocol errors.
iden	Performance Count records received from the Motorola’s iDEN equipment via a file-based interface with the mediation system.

System Backbone and Process

System backbone

This flow diagram shows major NTP functions in the center. Some *Oracle* databases are shown on the left and some system outputs are shown on the right.



Summary of system backbone processes

These points summarize the processes illustrated in the above illustration.

- Converting
  - The CFIM conversion and storage subsystem collects CIMs from the REs of the network under analysis.
  - The CIMs are converted into CFIMs by application of the conversion algorithms against fields in the CIM and by use of the reference data in the database.
  - The CFIMs are stored in the database.
- Thresholding and alerting
  - Counts of RE and FDC (final disposition code) combinations, or other combinations, are forwarded to the thresholding and alerting subsystem.
  - The thresholding and alerting subsystem increments and compares the counts against thresholds.
  - Periodically, the threshold crossings are fed into the alert algorithm in order to generate alerts, to correlate into the trouble-tracking Alert Case (ACASE) records.

Entity Roles

Roles and architecture

As system administrator, you deal with network "architecture" as seen by NTP. You need to understand how various entities may play different roles as:

- Reporting entity (RE)
- Distant entity (DE)
- Reporting STP
- Distant STP
- Related entity.

Point of view

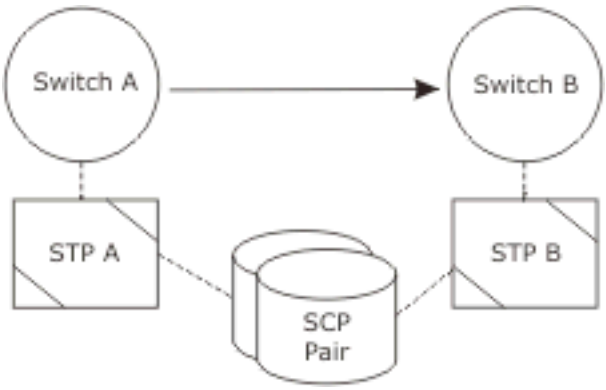
To understand these terms, you must use the REs point of view.

Often the RE is the call originating entity, and the DE is the call destination entity, but that is not always the case.

Example: See the following two diagrams and the accompanying scenarios.

Diagram 1

Use this diagram with the next Scenarios 1 through 3.



Scenario 1

Switch A attempts to reach switch B and encounters an NCA (no circuit available) condition. Find output shows the following :

Reporting Entity	Home entity's STP	Distant entity's STP	Distant entity	Call direction	Related entity	Related direction
Re	Rs	Ds	De	D	Related	R
Switch A	STP A*	STP B*	Switch B	O	-	-

Scenario 2

Switch A attempts to reach the SCP pair and gets a timeout. Find output shows the following:

Reporting Entity	Home entity's STP	Distant entity's STP	Distant entity	Call direction	Related entity	Related direction
Re	Rs	Ds	De	D	Related	R
Switch A	STP A*	STP B*	the SCP pair	O	-	-

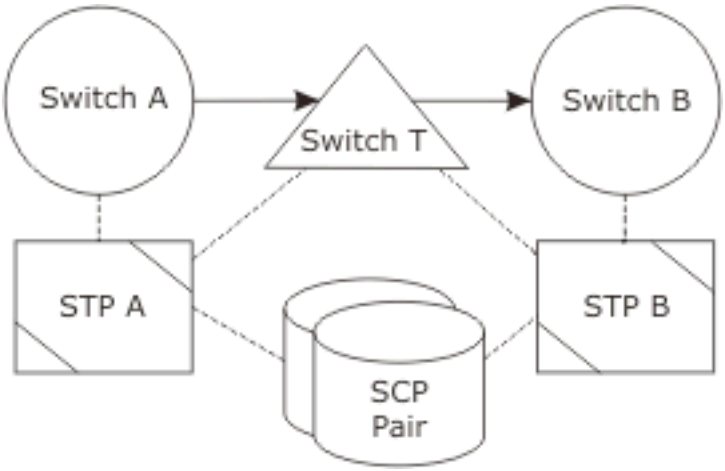
Scenario 3

Switch A misrouted information to switch B, and switch B issued a vacant code message. Find output shows the following.

Reporting Entity	Home entity's STP	Distant entity's STP	Distant entity	Call direction	Related entity	Related direction
Re	Rs	Ds	De	D	Related	R
Switch B	STP B*	STP A*	Switch A	*I*	-	-

Diagram 2

Use this diagram with Scenario 4.



Scenario 4

Switch A attempts to reach switch B via tandem switch T. Switch T encounters a no circuit available condition. Find output shows the following:

Reporting Entity	Home entity's STP	Distant entity's STP	Distant entity	Call direction	Related entity	Related direction
Re	Rs	Ds	De	D	Related	R
Switch T	STP A*	STP B*	Switch B	*O*	Switch A	*I*

Important! In all four scenarios, STP A* and STP B* mean the STP would be reported if the FDC indicates a signaling problem.

Files and Databases

Overview

Purpose

Background

NTP and its data reside as a collection of files in a single file system, the location of which is specified at install time.

Default NTP home directory

The default NTP home directory is */lucent/ntp*, although other customized locations are possible.

The NTP directory tree includes executable files, ASCII data files, and binary database files:

- Files
  - Hold NTP software and some reference data.
  - Are viewed and manipulated with shell-type commands, such as **`vi`**, **`cat`**, **`mv`**, **`cp`**, and **`del`**.
  - Are organized into directories, which you can visit by using the **`cd`** command.
- Databases
  - Hold surveillance data and most reference data.
  - Are viewed and manipulated with *Oracle* database commands and **`dbedit`**.
  - Are not organized into directories.

Contents

Oracle Databases

Purpose

Database storage makes possible quick and easy manipulation of data, including:

- Reference data, such as thresholds and network architecture
- Surveillance data, such as CFIMs and alert cases

Important!

- In the GUI, you see databases called "system tables" and "user files." While a database can be thought of as a table, calling a database a file could cause confusion, since files and databases are two different ways to store data.
- NTP uses *Oracle* software release 10.2.

Reference

Database tables are explained in the following places:

Reference	Explains
Chapter 3, “Reference Data Tables”	• How to use tables, including how to: • Use the **`describe`** command to get table explanations. • Use the **`dbedit`** command to add, modify, or delete records. • Audit tables.
Chapter 4, “Add Network Elements”	How to accomplish tasks that require adding, modifying or deleting records, including: • Adding a switch. • Adding an FDC.
Appendix A, “Reference Database Tables”	All reference tables and their fields. These are used primarily by system administrators.
Appendix A, "Surveillance Database Tables", in the *BB-GUI User's Guide*.	All surveillance tables and their fields. These are used primarily by network analysts.

Application Directory Structure

Application environment variables

NTP defines variables for many of the file systems and directories described here. These variables are available in the user environments of some logins (such as **ntp**) created when the system is installed. The tables in this section list the variable names as well as the file system and directory names to which the variables correspond.

Application environment variables in documentation

- *Input*. Throughout the user documentation, NTP environment variables are shown in pathnames and command lines.

  In almost all cases where input is required, you can enter either the actual path or the appropriate variable. For example, you can change to the /lucent/ntp/snas directory by entering either of the following:

  cd /lucent/ntp/snas

  cd $SNASDIR

  Regardless of the location of the NTP home for your installation, you can change to the NTP home directory by entering **cd $SNASDIR**.
- *Output*. Examples of output throughout this documentation assume that the NTP home is /lucent/ntp/snas.

Application directories

This table describes the directories under $APPLROOT.

Directory Name	Description	Environment variable
/lucent/ntp	Contains NTP software and database tables. Note that this file system is created by NTP installation scripts to hold NTP software.	$APPLROOT
/lucent/ntp/snas (default)	Contains subdirectories for NTP programs and shell scripts (see "snas directory" (p. 1-34)). Also known as the NTP "application home".	$SNASDIR (also $APPLHOME)
/lucent/ntp/dbf	Contains binary database files that comprise the various tablespaces used by the *Oracle* database. These files are often very large. See "Monitor Oracle Database Size" (p. 10-13) for information on preventing this directory from growing too large.	$DBFDIR
/lucent/ntp/ logdat	Contains error and event logging files.	$LOGDATA

Directory Name	Description	Environment variable
/lucent/ntp/oracle	Contains the installed base of *Oracle* RDBMS executables and non-application specific files.	$ORACLE_HOME
/lucent/ntp/oraexport	Used for importing and exporting *Oracle* tables.	$ORAEXPORT
/lucent/ntp/oralogs	Contains *Oracle* error log files.	$ORALOGS
/lucent/ntp/snas/install	Contains the installation software.	INSTALLDIR
/lucent/ntp/snas/install/log	Contains installation log files.	LOGDIR
/lucent/ntp/wgui	Contains BBGUI files.	$WGUIDIR
/lucent/ntp/<3rd_party>	Contains all the 3rd party software	<name>_HOME, for example APACHE_HOME

snas directory

This table describes the most important directories under the $SNASDIR directory (see $SNASDIR in "Application directories" (p. 1-33)):

Directory under $SNASDIR	Description	Environment variable
/appl	Subdirectory for NTP-specific files and executables. Contains data which does not change after an installation (other than patches).	$APPLDIR
/appl/bin	Contains utilities made public to you via the shell-level interface. These include *sui* (shell user interface), *dbedit, add_ntpuser, del_ntpuser, archive,* etc.	$APPLBIN
/database/sql	Contains SQL scripts required to initialize the product after an installation.	-
/database/schema	Contains scripts required during installation to create the database schema and prepopulate tables.	$SCHEMA_DIR
/appl/etc	Contains scripts used by the operating system cron utility and scripts intended for use by your NTP support organization.	$APPLETC

Directory under $SNASDIR	Description	Environment variable
/appl/init	Contains non-database related initialization files.	-
/appl/init/conv	Contains converter initialization files.	-
/appl/log	Contains the logger configuration files.	$LOGROOT
/control	Contains Oracle control files.	-
/model	Contains models or templates of files which you customize. The subdirectory structure closely follows that of the user subdirectories in order to allow NTP to first search a user directory and, if necessary, default to the corresponding model directory.	$MODELDIR
/model/misc	Contains miscellaneous templates not covered by the other subdirectories under the model directory, including cron model files.	-
/model/help	Contains the source for the fdchelp RDBMS table (for example, the *4ESS FHC Handbook*).	-
/snas	The home directory for NTP. (NTP login)	$HOME
/user	Contains user data managed by the NTP system administrator.	$USERDIR
/user/univ	Contains filter scripts for native CIMS (NCIMs) associated with "universal" type conversions.	-
/work	Contains data created and managed by NTP while it is running (including the RDBMS).	$WORKDIR
/work/boot /work/run	The boot and autonomous process run directories are created here as needed by the initialization process. Also, initialization output and other created files are created here. Trace output files are placed in subdirectories here. The BOOTLOG and INITLOG files are very useful for watching NTP initialization and basic status.	-
/work/tmp	Temporary files created while NTP is running are created here. This directory is automatically cleaned out as part of NTP startup.	-

Application Software Files

Purpose

Application software is what runs NTP.

Find your software release

If you call your NTP support organization with a problem, they may need you to tell them your NTP release. To get this information:

- on the NTP host, enter **`cat $SNASDIR/Release`**
- on the BBGUI, on any screen, right-click in an area of white space and select About Client from the pop-up menu.

Your screen may also list additional information about the last installation, such as any patch software installed or an operating system upgrade.

Maintenance releases

Consult your NTP support organization before installing *HP* or *Sun* maintenance releases on your NTP host machine.

Software loads

When you receive Alcatel-Lucent software or any other type of software from any vendor, please call your NTP support organization before you install it on the NTP host machine.

Important! We do not recommend that you load any software unless you first check with your NTP support organization.

CIM Data

Overview

NTP converts raw CIM into CFIMs, which are stored in the CFIM database table. Raw CIM data is stored as text in the CIM database table. CIM data is useful for viewing data not stored in CFIMs.

Please note that CIMs are stored in database files and handled just like any other chronological data with regard to backup and recovery, performance, access, and administration.

Hint: For information about CIM I/O, see "Thresholds" (p. 1-18) *and* Chapter 5, "CIM Source Administration".

CIM storage

Because CIM data takes a lot of storage space, by default CIMs are stored for a shorter length of time than CFIMs.

Administrative Tools and Routine Tasks

Overview

Purpose

The section is a cross-reference that identifies system administration tools you use and tasks you routinely perform, and tells where they are documented.

- "Administration Tools" (p. 1-39) describes the types of NTP commands you use for administrative tasks.
- The following sections break down tasks by general type:
  - "System-Level Tasks" (p. 1-40)
  - "User-Related Tasks" (p. 1-41)
  - "Tasks Affecting Output" (p. 1-42)

Contents

Administration Tools

Overview

System administration tools include commands, reports, and other useful items. There are two groups of commands.

- Standard operating system shell commands
- NTP commands, which are either:
  - SUI commands
  - Other (non-SUI) commands

SUI commands

Some NTP commands run from the operating system shell must be preceded by **sui**, as in: **sui find source=*dbname***

Please note that the BB-GUI functionality supersedes these commands for end users. System administrators may still, as in the past, use the command line for **sui** commands.

Hint: See Appendix B, "SUI Commands" *for information on the various sui commands.*

Non-SUI commands

Some NTP administrative commands run from the operating system shell do NOT require **sui**, such as **add_ntpuser** or **dbedit**.

Historically, these commands have never been available through end-user interfaces.

Non-SUI NTP commands are discussed as needed in procedures in various sections of this book. See the index to find the location of information on a particular command.

Privacy Policy File

NTP provides a "P3P" file that contains NTP's privacy policy (including a cookie acceptance policy) in .xml format. This file allows browsers to query the privacy policy and compare it to the security settings in the browser itself.

- To view the file on the BB-GUI using *Internet Explorer*, select View > Privacy Statement.
- To view the file on the BB-GUI using *Mozilla* or *Firefox*, select View > Pageinfo > Privacy.
- To edit the file to add local contact information, use a text editor to edit */lucent/ntp/wgui/html/w3c/p3p.xml*.

System-Level Tasks

Purpose

This table lists tasks that may require touching hardware, installing end-user software, or monitoring NTP.

Task	Use	References
Backup and restore	Host computer's backup and restore	Appendix C, "Application Backup and Recovery"
Install client software Install and configure for BB-GUI and Pattern Painter users.	Installation CD-ROMs or web-based installation files	• "Install Client Software for the BB-GUI" (p. 6-62) • "Uninstall Client Software for the BB-GUI" (p. 6-71)
Sources Manage links to sources: • TSMs (*5ESS*, 1A *ESS*, or *DMS* switches) • CPs (*4ESS* switches) • Other sources	• TSM menus • CP commands	• Appendix D, "Set Up 8925 Integrated Service Assurance" • *CP Administration and O&M* • Chapter 5, "CIM Source Administration"
Monitor the system	System logs	Chapter 10, "Routine Monitoring" (see the table in "Monitoring Recommendations" (p. 10-3))
Monitor reference data synchronization (only if refsynch is used)	Commands, output, and dbedit procedures associated with RDS utilities	"RDS task overview" (p. 12-4)

User-Related Tasks

Purpose

This table lists tasks affecting users (both analysts and administrative users).

Task	Use	Reference
Users, add or remove • NTP host user logins • BB-GUI administrator and user IDs	• **`add_ntpuser`** and **`del_ntpuser`** commands • Web User Administration and Web User Information pages	• "Add and Delete NTP Users" (p. 6-6) • "Add and Delete BB-GUI Users" (p. 6-33)
Commands available to persons in restricted shell	link or copy commands to *$USERDIR/rbin*	"Restrict User cron Functions" (p. 7-61)
BB-GUI, customize • Table layouts and saved searches • BB-GUI attributes • Links to customer-defined information on local practices	• BB-GUI interface • Assistance from your NTP support organization • files in *$APPLROOT/wgui/html/info/en/custfiles*	• "Create BB-GUI System Table Layouts and Saved Searches" (p. 9-6) • "Customize BB-GUI Attributes" (p. 9-7) • "Maintain Local Support Links" (p. 9-10)
Pattern Painter, customize displays	*dbedit* pptemplate and pptemp_columns	"Customize Pattern Painter Displays" (p. 9-11)
cron, give restricted cron	shell references	"Restrict User cron Functions" (p. 7-61)
FDC groups, define, assign users to, change user assignment, and give users permission to switch among groups — see "Tasks Affecting Output" (p. 1-42).		
FDC help text, Column help text, Column Tooltips, add or modify	*mod_helptext*	"Manage Help Texts" (p. 9-18)
Network group or segment, define, assign users to, change user assignment, and give user permission to switch among groups— see "Tasks Affecting Output" (p. 1-42).		
Defaults for all users (such as fields on SUI output) that are set by environment variables.	**`admset`** command	"Reprocess CDRs" (p. 10-42)

Tasks Affecting Output

Purpose

This table lists tasks affecting output, including GUI data, error logs, and system console.

Output affected	Task	Method	Reference
All	*Databases*. Keeping reference databases up to date, including: • Owners, entity types, signaling, domains, signaling networks, service types, and so on. • Switches and other entities in the architecture tables • Digit-based and trunk group routing in the routing tables • Call final disposition in the fdc table and fdc translation tables • Customers in the customer tables. Also perform database audits to ensure consistency.		• Chapter 3, "Reference Data Tables" • Chapter 4, "Add Network Elements"
Find CFIM	*Check Rt field*. It may often need updating. For *4ESS* only. Note that Rt field is always "-" if you have no *4ESS* REs.	*dbedit* de2route, rarely rtarch too.	"Correct wrong or missing Rt values" (p. 4-53)

Output affected	Task	Method	Reference
Alert Cases	*Define busy alert cases*. Set CFIM count that determines if NTP calls an alert case busy (for expiration).	*dbedit* to change ALERTDEF table	Chapter 8, "Threshold Administration"
	Threshold. Adjust number of iterations of an LSP that must be done for soaking thresholds.	*dbedit* to change LSPDAYTYPES table	
	Link failure.	*setsys* to change IF1 and IF2	
	5-minute threshold minimum. 5-minute threshold for each of 48 load set periods.	Use Man_thresh_xx Table to populate min column.	
	Hourly threshold minimum. Hourly threshold for each of 48 load set periods.	Use Man_thresh_xx Table to populate min column.	
	Threshold sensitivity factor. Adjust sensitivity factor that moves automatic threshold level.	Use alertdef table to change sensitivity field	
	Weight factors. Assign values to thresholding weight factors.	*dbedit* to change ALERTDEF	

Output affected	Task	Method	Reference
Alert Cases, Trapalert	*FDC groups*. Determine which a user sees. • Define an FDC group • Assign one or some to a user, or grant all	• *dbedit* fdcgroup, fdcgroupmap, and fdcpermit tables • Web User Information page (BB-GUI) • **mod_fdcgrp** command • *dbedit* fdcpermit table	• "List FDC groups" (p. 7-18) • "Create an FDC group" (p. 7-19) • "Assign Users to FDC Groups" (p. 7-23) • *Group Manager, Chapter 7. Web User Information and Administration in BBGUI User's Guide*
	Network groups, segments. Determine which a user sees • Define a group, segment • Assign one or some to a user, or grant all	• *dbedit* netgroup, netgroupmap, netseg, netsegmap, and netpermit tables • Web User Information page (BB-GUI) • **mod_netgrp** command • *dbedit* netpermit table	• "List network segments and groups" (p. 7-33) • "Define Network Groups and Segments" (p. 7-34) • "Assign Users to Network Groups and Segments" (p. 7-42) • *Group Manager, Chapter 7. Web User Information and Administration in BBGUI User's Guide*
Find Linkalert	*CP-host last message time*. Number of Zero Message (ZM) intervals allowed to occur before NTP generates a Link Alert message	*setsys* to change ZM	Chapter 8, "Threshold Administration"

Output affected	Task	Method	Reference
Mass Call Alerts displayed on Alert Cases and Trap Alerts screens	*Screen FDCs*. Eliminate CIMs with specific FDCs from being counted for mass call alerts.	*dbedit* on Mc field of fdc table	• Output, see *BB-GUI User's Guide*.
	Threshold. Change the threshold that triggers a mass call alert.	*setsys* to change MCATHRESH See *Set Enhanced Mass Call variable*	• Enhanced Mass Call Alerting, see the *BB-GUI User's Guide*

2 Start and Stop

Overview

Purpose

This chapter tells how to:

- Verify whether the NTP software application software is running
- Start and stop the NTP application software on the NTP host
- Start and stop the *Oracle* software on the NTP host
- Verify whether the browser-based GUI (BB-GUI) is running
- Start and stop the BB-GUI.

This chapter also discusses:

- System time — which may need to be reset under certain circumstances.
- Cron jobs — which may be impacted by stopping the system.

Please note that this chapter does not discuss how to start and stop the NTP host computer. Refer to the appropriate vendor documentation for this information.

Reference: For how to monitor NTP startup and shutdown to see if surveillance data was lost due to unscheduled shutdowns, see "Monitor NTP Startup and Shutdown" (p. 10-15).

Contents

Verify Run Status

Verify NTP Run Status

Overview

The NTP software and the *Oracle* database must both be running for NTP to function. The **runstat** command verifies the NTP run status.

runstat command

To verify that the host-based NTP software and *Oracle* database are running, enter **runstat** and check the output.

Syntax

runstat

There are no options or arguments for this command.

Oracle and NTP running

The following output from the **runstat** command shows that the *Oracle* database and the NTP software are both running (where *application* is NTP):

```
The Oracle RDBMS is running

The application initialization of boot processes is running

The application initialization of autonomous processes is running

The application software is running
```

Oracle running NTP down

If NTP is not running, runstat output includes the following lines:

```
The application initialization of autonomous processes is not
  running

The application software is not running
```

Oracle and NTP down

If the *Oracle* database and NTP are both down, `runstat` output contains the following lines:

```
The system is unavailable. Please see your System Administrator.
```

If runstat fails

NTP has monthly log files that track manual and automatic system startups and shutdowns. The system also logs more detailed startup and shutdown information for NTP, *Oracle* , operating system, and CP processes (if your system uses a CP source). If runstat fails, these logs can provide system status information. See “Monitor NTP Startup and Shutdown” (p. 10-15) . We recommend you check these logs before contacting your NTP support organization for software problems.

Verify BB-GUI Run Status

Overview

The **wgui_stat** command verifies the run status of the BB-GUI software and associated web server processes.

wgui_stat command

To verify the run status of the BB-GUI, enter **wgui_stat** and check the output.

Syntax

wgui_stat

There are no options or arguments for this command.

Output

You see output resembling the following, which contains:

- a list of running servers
- a page server process listing reflecting activities of BB-GUI users.

```
event-channel is running
gatekeeper is running
ldap is running
web server is running
osagent is running
Actuate server is running
Page servers processes are running:

ntp     /lucent/ntp/wgui/bin/TrapAlertServer

ntp     /lucent/ntp/wgui/bin/TrapServer

ntp     /lucent/ntp/wgui/bin/AlertCasesServer
```

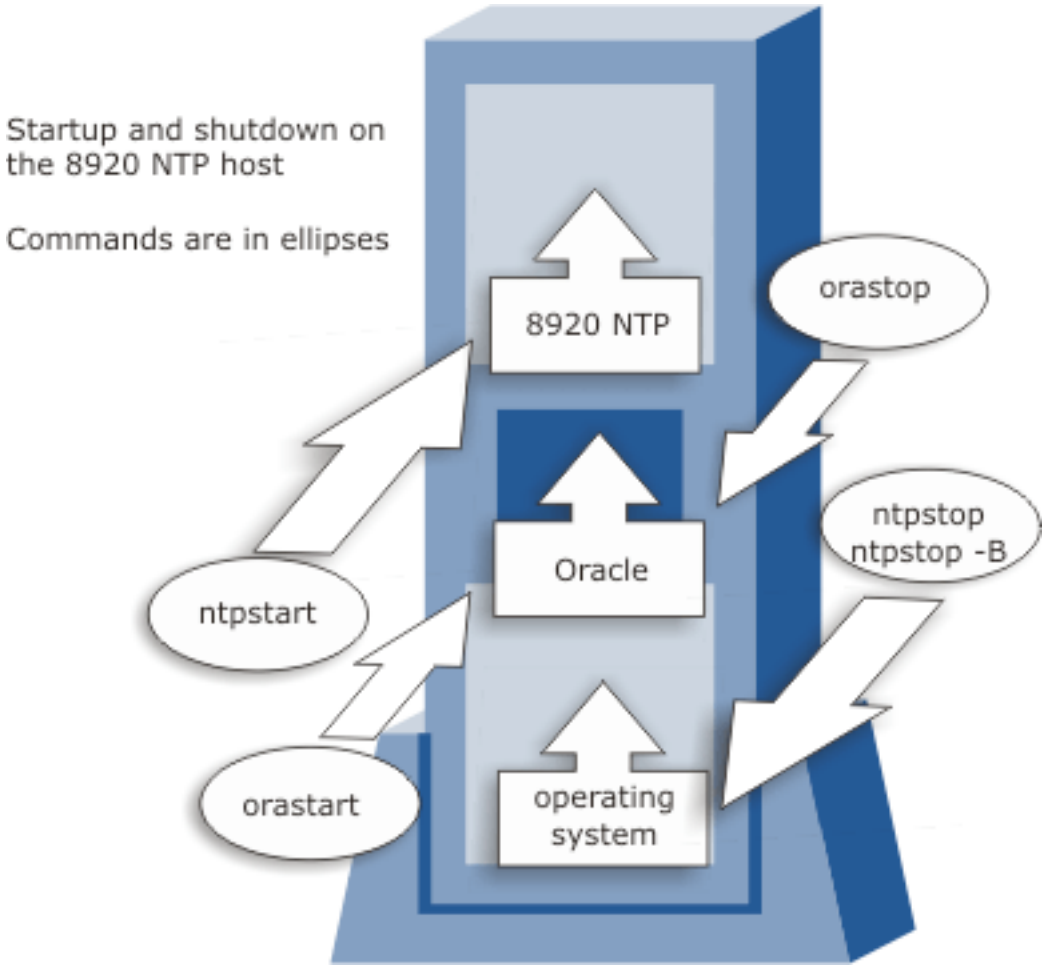
Start

Start NTP

Overview

The NTP software and the *Oracle* database must both be running for NTP to function.

This illustration shows startup and shutdown of the *Oracle* and NTP application software on the NTP host:



Start host-based NTP software

Procedure

Use this procedure to start the host-based NTP software:

1 Log on the NTP host as **ntp**. (You must be logged on as **ntp** to proceed.)

2 Enter **ntpstart**

There are no options or arguments for this command.

3 Enter **runstat** to verify that the system is running.

Reference: See "Verify NTP Run Status" (p. 2-3) for information on **runstat**.

If output from the **runstat** command still shows the software as down within ten minutes of running **ntpstart**, consult the *$WORKDIR/run/INITLOG* to troubleshoot. See "Monitor NTP Startup and Shutdown" (p. 10-15) for more information.

END OF STEPS

Start host-based Oracle software

Purpose

Use this if the *Oracle* software needs to be started without having NTP running (e.g., during maintenance).

Procedure

Use this procedure to start the host-based *Oracle* software.

1 Log on the NTP host as **ntp**. (You must be logged on as **ntp** to proceed.)

2 Enter **orastop**

3 Enter **orastart**

4 Enter **runstat** to verify that the system is running.

Reference: See "Verify NTP Run Status" (p. 2-3) for information on **runstat**.

END OF STEPS

Start BB-GUI

Purpose

You can stop and restart the BB-GUI processes while the NTP application software continues to run on the NTP host. The command to start the BB-GUI affects the:

- Web server
- LDAP server
- CORBA processes.

wgui_start command

The wgui_start command starts the BB-GUI.

Syntax

wgui_start

There are no options or arguments for this command.

Procedure

Use this procedure to start the BB-GUI.

1 Log on the NTP host as **ntp**. (You must be logged on as **ntp** to proceed.)

2 Enter **wgui_start**

3 Enter **wgui_stat** to verify that the system is running.

Reference: See "Verify BB-GUI Run Status" (p. 2-5) for information on **wgui_stat**.

END OF STEPS

How Users Access the NTP Interface

Access

Users can access NTP by multiple methods. Administration may be necessary depending on the method.

Reference:

- For how users start up NTP, see Chapter 2 in the *BB-GUI User's Guide*.
- For how you set up users, so they can start NTP, see Chapter 6, “Add or Delete Users” .

UI	Platform	Method	Note
BB-GUI	From PC, using browser	Administer web server and browser on PC.	Tell the user the URL of the BB-GUI Launch Page.
SUI	From the operating system command line	Give administrative users a login on the NTP host.	

Exit

Analysts exit the NTP by using the interface exit feature. See the *BB-GUI User's Guide*.

Stop

Stop NTP

Purpose

You must stop the NTP application and the *Oracle* database before you:

- Change system time (see "Advance system time on the NTP host" (p. 2-18))
- Install new host hardware, or new host or NTP software
- Reboot the system
- Run diagnostics on host hardware
- Do backups

Before you stop

Before you stop NTP, ask yourself:

- Is anyone logged on? (See "who command" (p. 2-12).)
- Are you approaching a load-set period (LSP) boundary?
- Are any cron processes running or about to run? (See "Cron" (p. 2-20)).

who Command

Purpose

Before you stop the NTP system, you need to know who is logged on so they can be warned that the system will be stopped. You can display a list of user accounts that are currently logged on via the who command.

who command

The operating system who command lists only users logged directly on the NTP host. It does NOT show users logged into the GUI.

Reference: See the output of the operating system man who command for details.

Side effects

- When NTP stops, all autonomous processes stop and connections to CIM sources (collectors) drop. No users can log on to enter NTP commands.
- Though the *Oracle* database is an essential part of NTP, you can shut down NTP without shutting down *Oracle*.
- If the system goes down while users are still logged on, you can expect effects like these:
  - If the database goes down, no commands can be run until it is again available. Commands running when the system goes down immediately terminate.
  - Users cannot run Trap Data or Alert Cases screen in update mode.
  - Users cannot run Find and get current data, since there is none. If the *Oracle* database is still running, users can search past data by specifying a time-related field in their search expression.

Cautions

Please note that:

- Before you stop the *Oracle* database, stop NTP. Otherwise, NTP will soon fail.
- Several times throughout the day, regular system activity takes place. NTP should not be shut down during these times:

Time	Activity
00:30	File cleanup; administrative report generation
01:00	Remove old news (info) files
23:00-01:00	Processing and generation of nightly performance reports
23:30-02:25	CP sampling rate reports arrive. (The times for these reports to be sent are set on the CP in local time. They may be changed by CP field support.)

ntpstop command

The ntpstop command stops the NTP application software running on the NTP host. When this command is executed, NTP stops for ALL users.

Syntax

ntpstop [-B] [-y] [<grace>]

Parameter	Function
-B	Stops NTP, the *Oracle* database, and various other processes if running. If only the *Oracle* database is running, stops *Oracle*.
-y	By default, the **ntpstop** command asks you to confirm that you want to stop the software. The *-y* option allows you to bypass this confirmation prompt. Note that this option eliminates your opportunity to halt the **ntpstop** command.
<grace >	Number of second until NTP stops (Default is 1). With the *-B* option, stops NTP, the *Oracle* database, and various other processes in the seconds specified. If only the *Oracle* database is running, only *Oracle* is stopped. Note that entering zero (0) in this field prompts an immediate shutdown.

Example: See the various stop procedures in this section for examples of command usage.

Stop NTP with or without stopping the *Oracle* database

Purpose

You may wish to stop the NTP application software with or without stopping the host-based *Oracle* software.

Check Oracle Status

Use the **runstat** command to determine if the *Oracle* software is running.

Procedure

Use this procedure to stop the NTP application software with or without stopping the host-based *Oracle* software.

1 Use the **who** command (see "who Command" (p. 2-12)) to see which users are currently logged on the NTP host and send a broadcast to notify all users that they should log off.

2 Log on the NTP host as **ntp**. (You must be logged on as **ntp** to proceed.)

3 Do one of the following

- To shut down NTP and NOT the Oracle database:

Enter **ntpstop**

- To shut down NTP AND the Oracle database:

Enter **ntpstop -B**

Reference: The system displays this message:

```
WARNING: You are about to shut-down the application software!!
Continue? [y or n]
```

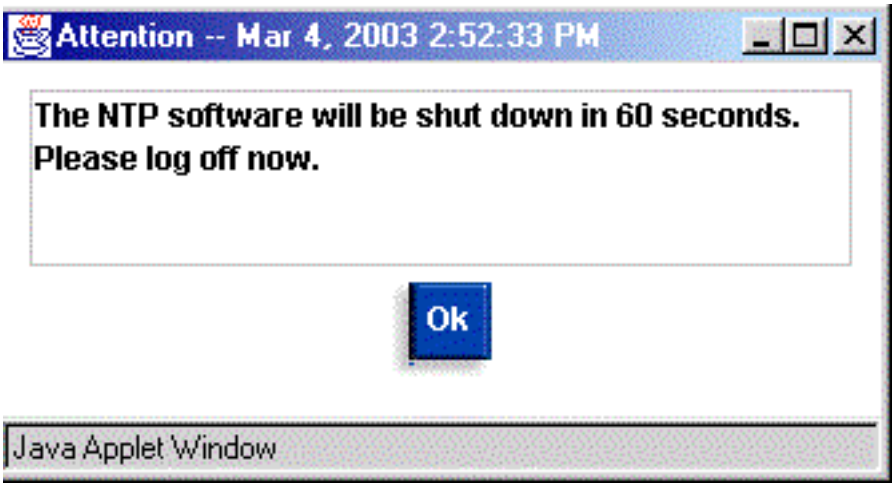
4 Enter **y**

After the system displays a message similar to this, all autonomous processes are stopped:

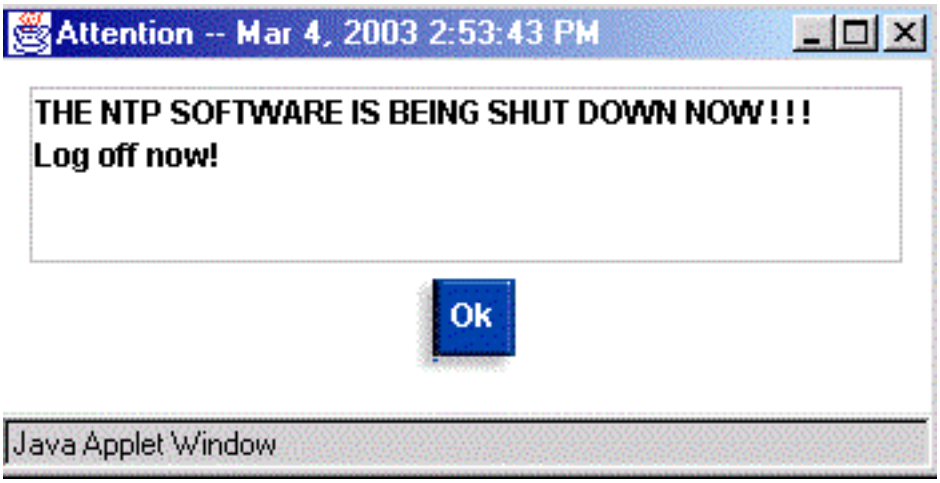
On the system:

```
08/15 13:48:24 Waiting 60 seconds for SHUT-DOWN completion...
08/15 13:49:24 SHUT-DOWN complete.
```

On the BBGUI:



and



END OF STEPS

Stop the *Oracle* database when NTP is stopped

Procedure

Use this procedure to stop the *Oracle* database when NTP is stopped.

1 Ensure NTP has been stopped. See "Stop" (p. 2-11).

2 Log on the NTP host as **ntp**. (You must be logged on as **ntp** to proceed.)

3 Enter **ntpstop -B**

Important! On some occasions, the *Oracle* database may continue to run because of configuration adjustments, problems encountered normally by *Oracle*, and so forth.

Result: The *Oracle* database should stop.

Did the *Oracle* database stop?

- If YES, you are done.
- If NO, then you must force a halt of the *Oracle* database with the *-a* (abort) option by entering **$APPLDIR/etc/orastop -a**

Result: The *Oracle* database stops.

END OF STEPS

Stop BB-GUI

Procedure

Use this procedure to stop the BB-GUI.

1 Log on the NTP host as **ntp**. (You must be logged on as **ntp** to proceed.)

2 Enter **wgui_stop**

Important! The **wgui_stop** command can take up to 30 seconds to complete before the operating system prompt returns. If all wgui processes were not successfully stopped, an error message is displayed.

3 Enter **wgui_stat** to verify that the BB-GUI is stopped.

Reference: See "Verify BB-GUI Run Status" (p. 2-5) for information on **wgui_stat**.

END OF STEPS

System Time

Advance system time on the NTP host

Purpose

Under normal circumstances, starting and stopping the NTP system does not require any change to the system time. Changing the system time should only be done when absolutely necessary.

You can set the system time forward on the NTP host, but NEVER set the time backward past the time when you stopped NTP. If your system time needs to be set back, contact your NTP support organization for assistance.

Important! Changing the system time while NTP is running can impair the way NTP stores time-stamped records, such as CFIMs and alerts. A change of time in either direction while NTP is running may cause damage to the record bases that is repairable only by a complicated procedure. If the time-stamping mechanisms suffer damage, contact your NTP support organization for recovery procedures (if possible, before restarting NTP).

Procedure

Use this procedure to set the system time forward on the NTP host.

1. Stop NTP and the *Oracle* database by completing the procedure in "Stop NTP with or without stopping the Oracle database" (p. 2-14).

2. From the login prompt, log on the NTP host as **`root`** (using the **`su -`** command).

3. Shut down the operating system to single-user mode.

   Reference: See documentation for your host operating system.

4. Set the time forward by using the **`date`** command of your host computer's operating system as described by the **`man date`** command.

5. Reboot the NTP host.

Reference: See documentation for your host operating system.

6 If necessary, restart NTP using the steps in "Start host-based NTP software" (p. 2-7).

END OF STEPS

Cron

Overview

Purpose

NTP uses the operating system cron utility to invoke periodic cleanup and preparation procedures. The cron utility requires special attention when the NTP software is stopped and started. You should be aware of the times when NTP-related cron jobs run if you plan a system shutdown, add other executables to a NTP-related crontab file, or create a user crontab file.

NTP-related crontab files

Your NTP host was installed with several crontab files.These files are in the */usr/spool/cron/crontabs* directory and include:

- "root crontab File" (p. 2-23)
- "ntp crontab File" (p. 2-24)
- "Other crontab Files (adm, oracle, and scp)" (p. 2-27)

You will probably never modify the adm, oracle, or scp crontab files.

You must log on the NTP host as root to modify the root crontab file and as ntp to modify the ntp crontab file. See "Start host-based Oracle software" (p. 2-8).

Reference:

- For how to give a user restricted access to cron, see "Restrict User cron Functions" (p. 7-61).
- See entries on cron and crontab in your operating system documentation for information about administering cron. Also see the comment lines in the ntp crontab file.

crontab file format

Each crontab file consists of lines of six fields each, separated by spaces or tabs. The first five fields are integer patterns that specify the time of day and the frequency of execution of the entry. An asterisk (*) signifies all legal values. Values can be inclusive ranges (two numbers separated by a hyphen) or comma-separated lists. The sixth field contains the command to be executed.

Reference: See your operating system documentation for specific information on crontab.

Invoking the correct shell

For shell compatibility, begin entries in crontab files with /bin/ksh -c, with the entry itself enclosed in double quotes (see the examples in "NTP-related crontab files" (p. 2-20)).

cron and your .profile

The cron utility does not run your .profile by default, so if there is something in a program invoked by cron that depends on your environment, you must explicitly run it in the crontab file. For example, add the following line, or set selected variables as required:

. $HOME/.profile

Managing cron output

The cron command sends standard output messages to your login as mail when it runs programs. If you do not wish to receive this output, add the string >/dev/null 2>&1 at the end of each command executed by cron or have the command redirect all error messages internally.

Example: **`command_in_crontab_file >/dev/null 2>&1`**

Contents

Modify crontab Files

Caution for upgrade and reinstall

Each crontab file entry created when NTP is installed is flagged with a comment line similar to this:

```
#Added by install_appl
```

Any changes you make to these flagged entries will be lost at the next install. However, any original entries you add to installed crontab files will be preserved at the next install.

Important! You should not edit crontab files with the vi or other editor. In your operating system documentation, note use of the **`crontab -e`** command necessary to modify crontab files.

root crontab File

Description

The root crontab file contains entries that perform the following types of functions.

- Clean log files
  These entries clean up log files.

  Important! You must be logged in as root to modify the root crontab file.

Reference: For more specific information about the contents of the crontab files, see the NTP Release Notes ("Software Release Notes and Third Party Software License Information" (p. xxviii)).

ntp crontab File

Description

Important! You must be logged in as ntp to modify the ntp crontab file.

The ntp crontab file contains entries associated with the following types of functions.

Reference: For more specific information about the contents of the crontab files, see the NTP Release Notes ("Software Release Notes and Third Party Software License Information" (p. xxviii)).

- File system space check

  This entry executes the NTP chk_space utility. This utility checks *Oracle* tablespaces and their associated data files. If the data file is getting too full, the utility adds a new data file for that tablespace and informs users specified in the notify table. (See "Monitor Oracle Database Size" (p. 10-13) ,"Alert notification" (p. 10-7) and "dialingcode Table" (p. A-56) for more information.)
- exp_db execution

  This entry executes exp_db, a NTP command that converts databases into files and stores the files in $ORAEXPORT (See "exp_db Command" (p. C-8) for more information on exp_db.)
- Error message collection

  This entry collects error messages for use by your NTP support organization and stores them in the $LOGDATA directory (see "Application logs" (p. 10-22) .)
- Administrative reports generation
  - Invokes the administrative report generation.
  - Cleans up unneeded Administrative Report files and the Event Logger files in $LOGDATA.
- RDS (refsynch) cleanup, check, and synchronization

  If your system will be using the RDS (reference data synchronization) feature (refsynch), during initial installation of your NTP, your NTP support organization will add appropriate entries in the ntp crontab file. Refsynch crontab entries can be the same on both hosts, as shown in the example below.

  Reference: See Chapter 12, "Reference Database Synchronization (RDS)" for more information on the refsynch feature that synchronizes reference data between a pair of NTP hosts.
- Cleanup of working sets

  This entry invokes a cln_usr script that cleans up orphaned temporary user files. These are the default files created during execution of find and ascreen commands such as ws, ws_prev, ws_view, and ws_view_prev.

- Cleanup of BB-GUI user files
  - Removes saved searches and table layouts that are older than the system default retention interval.
  - Prunes BB-GUI user histories stored on the BB-GUI server to a fixed number (see "User histories" (p. 9-8) for more information).
  - Creates a login $LOGDATA that shows what was removed (see "Monitor BB-GUI Cleanup" (p. 10-40)).
- CDR processing and garbage cleanup

  This entry executes a **`cln_bildts`** script that removes files every half hour from the garbage and processed directories used in CDR conversions, including:
  - IPDR
  - *AXE* TRADO
  - Lucent Softswitch
  - Consultant-configured
  - *GeoProbe*
  - *AXE* 10

  This script gets the directory names from entries in the Dir_list field in the "fileconfig Table" (p. A-76) .

  Reference: See "Sources for Configurable Conversions" (p. 5-40) for more information on these directories.
- Check space

  This entry determines how much space you are using and how much you are going to need in the future. Output from this entry can be lengthy, but will end with information such as this:

```
Total database growth required is 16968 MB

Total filesystem space available is 96370 MB
```

- Check tablespace size

  This entry looks for tablespaces that need to grow because they are becoming full. It then adds tablespace as necessary. Output is given only if tablespace is altered. This script runs hourly.

  Example output is as follows:

```
WARNING: CIM2 tablespace is getting full

Adding datafile for CIM2 tablespace

Tablespace altered.

Added /lucent/ntp/dbf/rcim.2.4 to tablespace cim2
```

- autotest tool

  The autotest tool provides a method of monitoring system status and health. It allows the user to create and configure their own tests.

  Reference: For more information, see "autotest Tool" (p. 10-10) .

- Creating new oracle database files

  The **chk_dfilesize** command in the ntp crontab is responsible for creating new oracle database files. At very high CIM rates, it may not be set to run often enough to keep pace with the incoming data. If that is the case, increase the frequency of execution.

  Contact your Alcatel-Lucent support organization for additional information.

Other crontab Files (adm, oracle, and scp)

Description

You should not need to modify the adm, oracle, and scp crontab files.

- adm crontab file
  The operating system populates the adm crontab file.
- oracle crontab file
  Entries are in the oracle crontab file.
  - Clean up the *Oracle* database ($ORALOGS and *Oracle* listener).
  - optimize system performance for current-day find.
- scp crontab file
  The scp crontab file is important in systems with the CP-on-host feature.

3 Reference Data Tables

Overview

Purpose

Procedures throughout this book update database tables that hold reference data. Those procedures refer you to this chapter for more information on some aspects of database editing, such as **`vi`** or **`dbedit`**. You might also use this chapter if you need to do table editing not covered by a procedure.

Contents

Introduction

Introduction To Database Tables

Reference versus surveillance tables

Reference data tables are distinguished from surveillance data tables as follows:

Each database table holds either	Description	Reference
Reference data	Reference data defines network elements. You use **dbedit** or other tools to modify these tables so NTP can run correctly.	Appendix A, "Reference Database Tables".
Surveillance data	Surveillance data appears on outputs. You do NOT **dbedit** surveillance data tables.	Appendix A of the *BB-GUI User's Guide*.

Important! Though you never **dbedit** surveillance data tables, analysts using the GUI can modify the acase table, as explained in Chapter 5 of the *BB-GUI User's Guide*.

Modify databases

Purpose

Reference data tables tell NTP how to run correctly. You sometimes use **dbedit** or other tools to update reference data tables.

Important! You update reference data tables so they will accurately do the following:

- Tell NTP what is in the network, including switches, STPs and SCPs.
- Tell NTP how to convert CIMs to CFIMs.
- Assign FDC groups to users.

Procedure

Modifying database tables involves the following steps:

1 To see what tables exist and what fields are in tables, use any of the following:

- Table or field helps (see "Table and Field Helps" (p. 3-9)), such as the **describe** command (see "describe Command" (p. 3-10))
- Information on the various tables in Appendix A, "Reference Database Tables"

2 Create an ASCII text input file in the format of the table you want to update. You can use an ASCII text editor (such as **vi** — see "Edit (vi) ASCII Files" (p. 3-13)) to type the file from scratch. But more often you will do the following:

- Use **sui find** to retrieve a database into an ASCII file (see "sui find for dbedit" (p. B-20)). To tailor retrievals, you can use the command's **search** parameter (see "Search Expressions in sui find" (p. B-29)).
- Use an ASCII text editor (such as **vi**) to modify the ASCII file (see "Edit (vi) ASCII Files" (p. 3-13)).

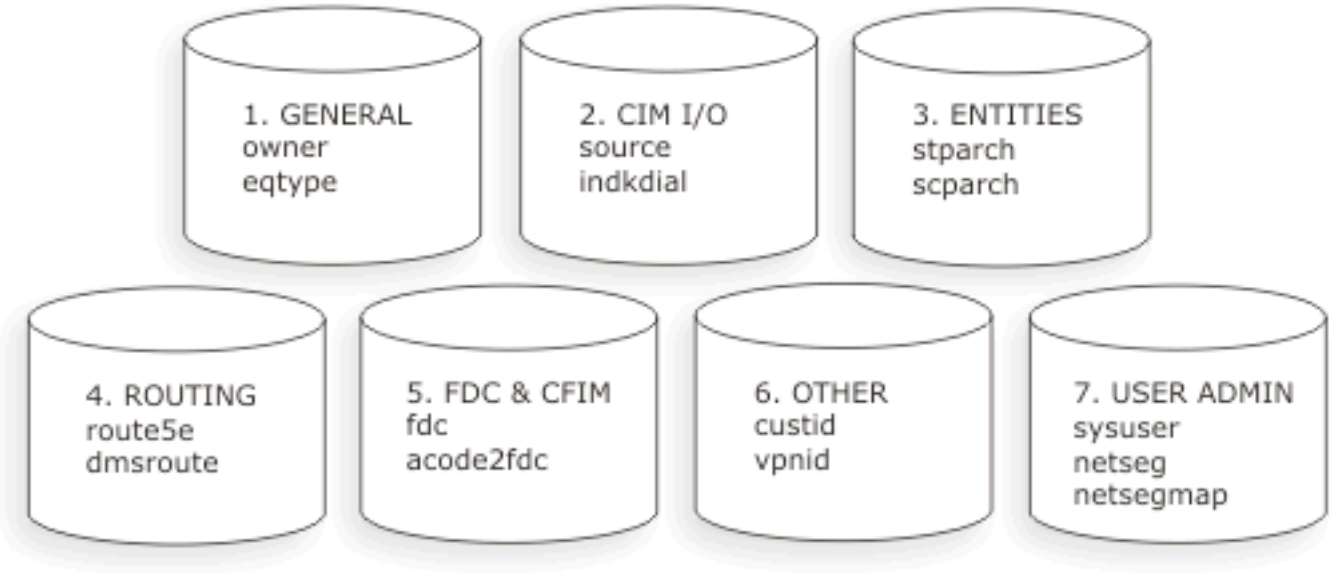
3 Use **dbedit** to use the ASCII file to modify the database (see "Dbedit" (p. 3-17)).

END OF STEPS

Tables

Groups of reference tables

Reference data tables fall into seven logical groups, illustrated here.



Reference: For the full list of tables in each group, and their installation order, see "Installation order summary" (p. 3-43).

Important!

- The illustration above does NOT include the surveillance data tables. For those, see the *BB-GUI User's Guide*.
- Some tables (both reference and surveillance) are for optional features. Typically, if you do not have a feature, you still see its tables, but they are ignored.

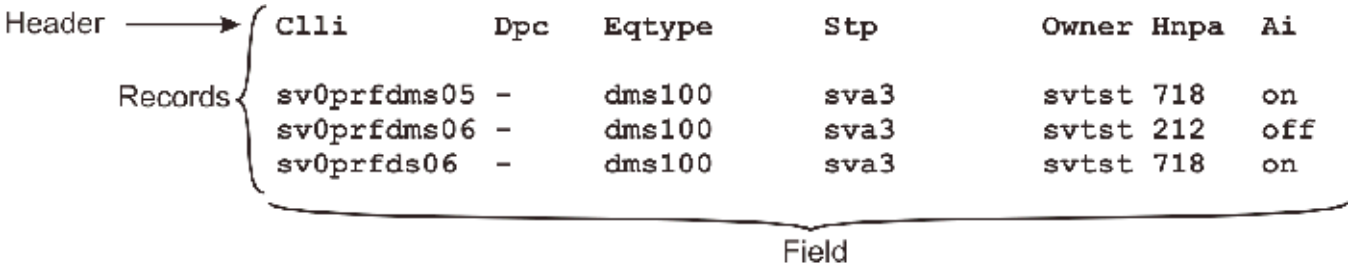
Records

Definitions

Each database table has:

- **`A header`**. It shows the field names.
- **`Records`**. Each line is a separate record, representing, for example, one switch, one FDC, or one user.
- **`Fields`**. Each record has two or more fields. Each field holds a value. Change values in fields in order to change an FDC, switch, and so on.

Example: In the swarch table, the first few records might resemble this:



How to see records

There are two ways to see records in tables.

- **`sui find`**. Use this command at the operating system shell (see "sui find Command" (p. B-18).)
- **`GUI`** Find. You do this from the BB-GUI. For how to do this, see the *BB-GUI User's Guide*.

Fields

Field types

Field helps tell you what type of data each field holds. Field types are either:

- **`String`** — alphanumeric.
- **`Set`** — a predefined set of strings.
- **`Numeric`** — digits.
- **`Date or time`** — digits giving date or time (on surveillance data only).

Field type matters in the following two cases:

- **`Add`**. If you are adding or modifying a field. For example, you cannot put letters in a numeric field.
- **`sui find`**. If you are using a search expression with the **`sui find`** command. For example, you cannot search a range for a string or set field.

Key fields

A key field (or fields) uniquely identifies each database record. Non-key fields give attributes.

The key field (or fields) are first in a record.

Each key field (or fields) must hold a unique value (or combination of values) among records in a table. Non-key fields can hold the same values.

Example: The key field for the swarch table is clli.

Key fields:

- Are noted in the field helps. For how to get field helps, see "Table and Field Helps" (p. 3-9).
- Require special consideration with the **`dbedit`** command. See information on input file rules in "Input file rules" (p. 3-20).

Null characters

Fields are never blank, but sometimes hold a null character, listed below.

Character	Seen in	In	Meaning
- (dash)	Any non-key field	Reference and surveillance tables	In surveillance tables, this means "does not apply" (for example, there was no related entity, so Related is "-" on Find CFIM) or unknown (for example, something was missing from a CIM). In reference tables, this also means "does not apply". However, you may also use it when you do not know what to enter in a non-key field. In this case, it may result in a "?" in a field in surveillance data, explained next.
? (question mark)	A few key and non-key fields	Some surveillance tables	The system tried to get a value from a reference table, but found nothing. In other words, you need to put something in some reference table. See "Shared Procedures" (p. 4-60) for how to fix these.
~ (tilde)	A few key fields	Some reference tables	Any (or ignore). To see if a field can use this, use a field help listed in "Table and Field Helps" (p. 3-9). *Example:* The acode2fdc table has four fields; acode, fname, FDC and error_origin. It maps combinations of values in first two fields (from DMS or 5ESS CIMs) to an FDC in the last field. If the first field holds X, and the second holds "~", and the third holds Y, it means X always maps to Y, ignoring the second field.

Important! To input a null field, you use two delimiters, such as ";;". The **`dbedit`** command then either tells you null is not permitted, or changes it to "-" or "~" in the table. This is explained in "Input file rules" (p. 3-20).

Table and Field Helps

Helps

The following tells where to find helps for reference tables and their fields.

To get table and field help in...	Use...
User documents	Appendix A, "Reference Database Tables"
Shell	The **describe** command (see "describe Command" (p. 3-10))
GUI	See the *BB-GUI User's Guide* .

Quick peek

If you just want to know a table's fields and their order, enter the following to list the header and one record.

sui find noheader source=table maxsave=1

Example: For the swarch table, enter

sui find noheader source=swarch maxsave=1

Which gives output resembling the following:

```
#Clli  Dpc Eqtype Stp Owner Hnpa Ai Ccd Ipaddress Description
00beileo22t -  - - att 000 off - - -
```

describe Command

Purpose

The describe command describes tables and their fields.

Syntax

describe [-a] [-n] [-c | -u | tablename [field]] [| pg]

Parameters

The describe command parameters are as follows:

Parameter	Function
-a	Describes tables and fields in alphabetical order. Without this parameter output is in default order, which begins with key fields.
-n	Omits table and field descriptions, and lists only the table and field names. Without this parameter, you get table and field descriptions.
-c	Describes tables and fields for all surveillance tables. (These are the databases you do not **dbedit** .) Typically, this parameter is used with **-n (describe -c -n)** to list just table and field names. Otherwise, output is overwhelming. If you enter **-c** with **-u** , **-u** is ignored.
-u	Describes tables and fields for all reference tables. This is the same as default (what you get if you omit **-c** and **-u**). Typically **-u** is used with **-n** (describe **-u -n** , which is the same as **describe -n**) to list just table and field names. Otherwise, output is overwhelming.
tablename	Describes fields for one table This is the most common usage of the **describe** command.
field	Describes one field in the table specified. Can be used only after a table name. If the field is not in the table, you get no output. Omit this parameter to see all fields.
| pg	A standard operating system pipe and **pg** command that enables you to see one page of output at a time. Press **Return** to go to the next page. Without this option, if the description contains many lines of output, they scroll up your screen and you see only the last page of output.

Important! If you use describe to see many tables, it takes a long time for them to scroll on your screen. To abort the command, press Delete.

Example 1

This example requests a description of the eqtype table and its fields.

```
$ describe eqtype
EQTYPE TABLE DESCRIPTION:

This table contains a list of equipment types known to the
system.  The table will be populated with the following
switch types at installation time.

(4ESS) (5ESS) (Operator Service Position Switch) (1A ESS)
(1A ESS Tandem) (1 ESS) (1 ESS Tandem) (2B ESS) (2 ESS) (3
ESS) (5GTE) (Ericson 10) (DMS 10) (DMS 100) (DMS 200) (DMS
250) (DMS 500) (Network Inbound Switch) (Private Branch
Exchange) (Traffic Operator Position System) (SCP) (NSCX)
(AUTOPLEX Mobile Switching Center) (Siemens EWSD) (summa
four) (Alcatel S1240) (Lucent Softswitch) (DMS MTX Mobile
Switching Center) (Nortel GSM Mobile Switching Center)

The administrator will be able to update the equipment types
in this table.

FIELDS:

_____________________________________________________________________
DESCRIPTION:
---=default=---
This field provides a description of the equipment type.
"-" is a valid value that indicates the field is not
applicable or there is no data available.  Field Type:
String of 50 mixed case printable characters.

_____________________________________________________________________
TYPE:
---=default=---
This field defines the equipment type (type).  This is a key
field in the eqtype table. Field Type: String of 8 printable
characters.

_____________________________________________________________________
VENDOR:
---=default=---
The vendor field contains the vendor (or constructor) name
of the RE.  "-" is a valid value that indicates the field is
not applicable or there is no data available.  Field Type:
String of 20 printable characters.
```

Example 2

This example requests the list of fields in the eqtype table, with no descriptions.

$ describe -n eqtype

```
EQTYPE TABLE:
        DESCRIPTION
        TYPE
        VENDOR
```

Edit (vi) ASCII Files

Definition

An ASCII file is a file you can list, create, edit or delete in shell—versus databases, which are not ASCII files, and can not be seen in shell.

Purpose

You need to know how to manipulate and how to use a text editor (such as vi) to edit ASCII files, since many procedures in this book ask you to do the following:

- sui find. Use sui find (see "sui find Command" (p. B-18)) to copy a database or records from a database into an ASCII file. (Or, you can use a text editor to create the ASCII file from scratch.)
- Text editor. Use a text editor to edit records in the ASCII file.
- dbedit. Use dbedit (see "Dbedit" (p. 3-17)) to modify, insert or delete the ASCII file's records back into the database.
- Remove. Remove the ASCII file after you are done with it (see **rm** in "Manipulate files" (p. 3-13)).

Manipulate files

Use this table for examples of how to manipulate or learn about ASCII files.

To do this (in shell)...	Enter...	Example...
Go to your home directory.	**cd $HOME**	There is no screen response, but you can use **pwd** to verify where you are.
See where you are in shell. List ASCII files.	**pwd** **ls**	If your home directory is named djd, you see: /home/djd If the files there are named temp1, temp2, and temp3, you see: temp1 temp2 temp3
See how many lines are in a file (the number of lines in a file equals the number of records retrieved from a database).	**wc -l file**	To see how many lines are in a file named temp, enter **wc -l temp** If there are 100 lines in the file, you will see: 100 temp (For an example of when you might use this, see **maxsave=1-100000_records** in the Parameters table .)

To do this (in shell)...	Enter...	Example...
See what is in a file (without entering the file via **vi**).	**cat file**	To scroll to your screen the contents of the file named temp, enter **cat temp**
Create an ASCII file from a database.	**sui find** with **> file** option	See the following parameter: "> *file*" in the Parameters table .
Create an ASCII file with the **vi** editor.	**vi file** (For using **vi**, see "Edit (vi)" (p. 3-14).)	To create a new file named temp, enter **vi temp** You are in an empty file with your cursor at the top, resembling this: ~ ~ ~ "temp" [New file]
Edit an existing ASCII file.		To edit an existing file named temp, enter **vi temp** You enter an existing file with your cursor at the top, resembling this: Here is a line of text in the file. Here is a line of text in the file. ~ ~ "temp" 2 lines, 72 characters
Remove an ASCII file.	**rm file**	To remove a file named temp, enter **rm temp**

Edit (vi)

Use this table for examples of using the vi editor once you are in an ASCII file. (To enter an ASCII file, see "Manipulate files" (p. 3-13).) The last two items tell how to get out of an ASCII file.

Important! Other options. There are many other vi options. To fully learn vi, you may need to take a class or use reference material.

To...	Do this...
Move your cursor one space or line at a time.	Press the arrow keys.

To...	Do this...
Page forward or back.	Hold down the **Control** key and press **f** or **b** (**Control-f** or **Control-b**).
Start entering text: • Before the cursor • After your cursor • On a new line below the cursor • On a new line above the cursor	Type letter: • **i** • **a** • **o** (lowercase letter o) • **O** (uppercase letter O)
Stop entering text (that is, get out of the text editing mode).	Press and release the **Escape** key. If you are not sure which mode you are in, do this, since it does no harm to press **Escape** when you are already out of the text editing mode.
Start a new line while entering text	Press the *Return* key.
Jump to the: • Next word • Previous word	Press and release the *Escape* key to make sure you are not in the text editing mode, and then: • Type **w** • Type **b** (Do not press the *Return* key.)
Delete a line	Press and release the *Escape* key to make sure you are not in the text editing mode, move your cursor to the line, and type **dd** (do not press the *Return* key).
Delete letters on the right	Press *Escape* to make sure you are not in the text editing mode, move your cursor to the first letter you want to delete, and repeatedly type **x** (do not press the *Return* key).
Copy and paste a line	1. Press and release the *Escape* key to make sure you are not in the text editing mode. 2. Move your cursor to the line you want to copy, and type **yy** (do not press the Return key). 3. Move your cursor to above where you want to paste the line, and type **p** (do not press the Return key).
Make global changes throughout the file	Use the global change option. *Example:* To change the word "off" to "on" throughout the file (where "off" is at the end of each line), press and release the *Escape* key to make sure you are not in the text editing mode, then type **:g/off$/s//on/gp** and press the **Return** key.

To...	Do this...
Exit an ASCII file (return to shell), saving your changes	Press and release the *Escape* key to make sure you are not in the text editing mode, then type :**wq** and then press the *Return* key.
Exit an ASCII file (return to shell), NOT saving your changes	Press and release the *Escape* key to make sure you are not in the text editing mode, then type :**q!** and then press the *Return* key.

Dbedit

Purpose

As outlined in "Modify databases" (p. 3-4), dbedit is the final step in the process for updating reference database tables. Run dbedit in shell.

Back up files for dbedit

Purpose

Make a backup file of any database table you are going to dbedit. To do this, enter:

```
sui find noheader source=table noheader delim='";"' maxsave=100000 >
   file
```

Example: To back up the swarch table to a backup file named hold_swarch, enter:

```
sui find noheader source=swarch noheader delim='";"' maxsave=100000>
   hold_swarch
```

Recover files after dbedit

Purpose

If a dbedit causes system problems, dbedit the backup file back into the database.

Tables you do not dbedit

This table explains when not to use dbedit.

Do not dbedit this table	Instead use	Reference	Notes
gtspec	**loadgt** command	Chapter 11, "Update the gtspec Table"	Use **loadgt** to load the gtspec table from a **dbedit**-compatible input file. (The **loadgt** command does special checking.)
sysuser (to add or delete users)	**add_ntpuser and del_ntpuser** commands	Chapter 6, "Add or Delete Users"	These commands add or delete NTP users from the host.

ASCII Files for dbedit

Purpose

dbedit uses an ASCII input file. The file holds records to either insert, update, or delete.

How to get input files

There are three ways to get an ASCII input file:

- Sui find. Usually, use sui find (see "sui find for dbedit" (p. B-20)) to create the file from a database, and then use a text editor (such as vi— see ("Edit (vi) ASCII Files" (p. 3-13)) to edit the file to reflect your changes.
- Type. Use a text editor (such as vi — see "Edit (vi) ASCII Files" (p. 3-13)) to create a file from scratch (rarely done).
- Script. Sometimes, get a file from another source, and then run it through your own shell script to put the fields in correct order, remove extra fields, add missing fields, and add delimiters.

Input file rules

Rules for input files are:

Rule	Explanation
One file per operation	One input file can be used to perform one update operation (on one database table). (You cannot use the same table to delete and update or delete and insert at the same time.) The four operations are: • Insert • Update • Both update and Insert • Delete This means, do not put records for different purposes in the same input file. For example, do not mix records to be inserted with records to be deleted.
One line per record	Each line (each return) is a record. Line wraps are ignored. Exceptions are the record with help texts which contains consisting of multiple lines of text for on-context help, See the **-r** option in "dbedit Command" (p. 3-22). A special record separator is required in an input file. See also "Manage Help Texts" (p. 9-18).
Blanks and # okay	Blank lines and lines starting with # are ignored by **dbedit**.
Field order matters	Use default field order. For how to get a list of a table's fields, see "Table and Field Helps" (p. 3-9).

Rule	Explanation
Use delimiters	Use semi-colons between fields (the **sui find** delim parameter inserts these when creating a file. Note that if you do not do this, each space and tab is seen as the start of a new field. If a field must contain a semi-colon, you can use another character as a delimiter, such as a colon (:) or Control-a.
Use key fields for deletes	If the records in an input ASCII file are to be deleted from a database, you need only key fields. Other fields are ignored. *Example:* The key field for the swarch table is clli. To delete this record from swarch enter **sv0prf01537;-;dms100;svae;svtst;703;off** The input file can hold this record (notice that the delimiters can be omitted): **sv0prf01537**
Use all fields for inserts or updates	If the records in an input ASCII file are to be inserted or updated in a database, you need all fields (but you can use ;; to specify blank fields). *Example:* To add a switch to swarch, enter, for example: **sv0prf01537;;dms100;svae;svtst;703;off**
Use ";;" for blank fields	If you want a field to be blank, use two consecutive delimiters (;;). • For non-key fields, **dbedit** changes ";;" to "-". • For key fields, IF blank is permitted, **dbedit** changes ";;" to "~" tilde). See null characters "-" and "~" in "Null characters" (p. 3-8).
No update of key fields	You cannot update a key field, since that would mean re-identifying a record. Instead, to change a key field, you must: 1. Delete the record from the table. 2. Insert a new record. Remember, a key field must be hold a unique value. A set of key fields must hold a unique combination or values.

dbedit Command

Purpose

dbedit is the final step in the process for updating reference databases. Run dbedit in shell.

Reference: For how to respond to dbedit errors, see "Correct dbedit Errors" (p. 3-27).

Syntax

```
dbedit operator -i -u -iu -d -t table -f input_file [ -o output_
file ] [ -l error_limit ]  [ -s "delimiter" ] [ -r "record_
separator" ]
```

Example: To update the swarch table, using an input ASCII file named temp, and with semi-colon as delimiter, enter dbedit -u -t swarch -f temp -s ";"

Parameters and functions

Here are the parameters for the dbedit command:

Parameter	Function
operator	(Required) Tells what to do with the input file. Options are: • -i The insert option reads records (one line = one record) from the input file and inserts them into the specified database table. This option is for adding NEW records into the database table. Records are rejected if they duplicate existing records (determined by matching key fields). • -u The update option reads records from the input file and uses them to replace their existing counterpart in the specified database table. This option is for changing information in existing records. Records are rejected if they do not already exist (that is, if a match cannot be found for the key fields in the record). You cannot use -u if all fields in a table are key fields. • -iu The insert or update option reads each record from the input file and, if the record's key field values: – Are in the database table, updates the matching record – Are NOT in the database table, inserts the record as new This option is for entering batches of records that are either new or modifications of existing data. Records are rejected only when they have invalid data. You cannot use -iu if all fields in a table are key fields. • -d The delete option reads records from the input file and deletes any matching records in the database table you specified. Records are rejected if a match cannot be found for the key fields, or if other database records have a dependency on the record being deleted.
`-t table_name`	(Required) Names the database table being updated.
`-f input_file`	(Required) Names the ASCII input file.Enter the name of the input file containing the records for updating this database table.
`-o output_file`	(Optional.) Name the output file in which error messages and rejected records will be written. The name must be different from the name of the input file. If you do not specify an output file name, an output file is created with the name *dbtablename*.error in the current directory (for example, for "-t swarch", this would be swarch.error).

Parameter	Function
-l error_limit	(Optional) Enables you to specify a limit of the number of errors to be found before **dbedit** stops retrieving records. Default is 1000. The limit is 10,000. All unprocessed records are appended to the end of the output file. For large input files (such as for routing tables), you may want to set this higher than 1,000.
-s "delimiter"	(Required) Defines the single character that the database editor is to interpret as the delimiter of fields in an input record line. (Actually, this is optional, but if omitted, the default delimiter is a space or tab character, which can cause problems.) To be consistent with what is suggested for the **delim** parameter of the **find** command (see the following parameter **delim=**' ";" 'in the Parameters table), use semi-colon.
-r "record_ separator"	Required when editing tables with multi-line records. Specifies a single character that separates one multi-line record from the next. Select a character that you do not need to use in text. Use of ^A (**Control-a**) for the record separator is recommended. See "Manage Help Texts" (p. 9-18) for the most common use of this option. If you use the **-r "record_separator"** option, you must also use the **-s "delimiter"** option.

During and after dbedit

During dbedit

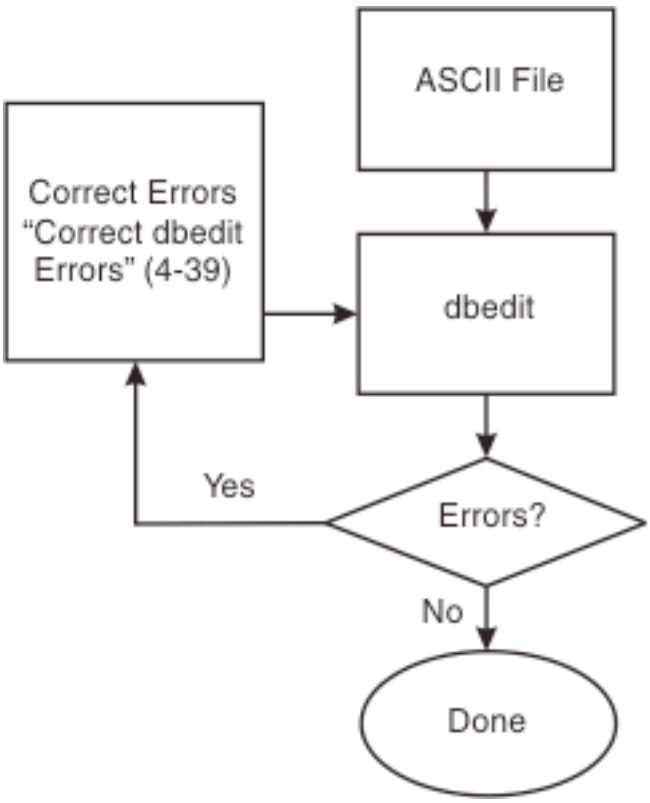
While dbedit is running:

- No double-dbedits. If you attempt to dbedit a database while a dbedit is running on that database, you may cause logical conflicts. (These will be reported as errors in the error file. That file is discussed in "Correct dbedit Errors" (p. 3-27).)
- No stop. The Delete key is disabled during processing.

  Important! You can limit the processing time by using smaller input files or by specifying a low error limit parameter (-l) with dbedit. Processing continues until the error limit is reached or all records in the file are processed.

Work Flow

This is the work flow after you enter dbedit.



sui find after dbedit

Using sui find to display records is a good way to verify that the dbedit operation you performed did in fact make the changes you want to the NTP reference data. See "sui find for dbedit" (p. B-20).

When changes take affect

Database table edits take affect either:

- Immediately. When you run successfully run dbedit.
- Plus 5 minutes. Tables used for CIM-to-CFIM conversion (including routing and customer tables) may require an additional 5 minutes before they affect CIM-to-CFIM conversion. This is because conversion changes require the tables to be loaded into shared memory, which happens every five minutes when a ldlkup script automatically runs.

Correct dbedit Errors

Purpose

When you run dbedit with no errors, no error file is created. But, if any records fail to insert, update, or delete, they go into an error file. The file has two purposes:

- It tells you why each record failed dbedit.
- It is an input file, to correct using a text editor (such as vi), and then to again run with dbedit.

Where the error file is

The file is in the directory where you ran dbedit (typically your home directory). By default, it is named with the table name plus ".error".

Example

- If you entered: dbedit -u -t swarch -f temp -l 25 -s";" The error file would be the default swarch.error
- If you entered the following, with the -o option: dbedit -u -t swarch -f temp -o tempout -l 25 -s";" The error file would be tempout.

  Important! If you used default, you must rename the error file before dbedit. For how and why, see Step 2 in the procedure "Correct dbedit errors" (p. 3-30) .

What is in the error file

Three things are in the error file:

- Comments. Tell how to fix rejected records. You do NOT need to delete these before running dbedit on the error file. These start with "#", telling dbedit to ignore them.
- Rejected records. Use a text editor (such as vi) to fix these, according to error messages. Then run dbedit on the error file.
- Records not yet processed. If you used dbedit's error limit option (-l), then dbedit stopped after the number of failed records you specified (default is 100 failed records). After the limit is reached, records not yet run are put into the error file, so you can run them from there.

Although the error file shows errors for multiple lines (up the number of lines specified by dbedit's "-l" parameter, the error file shows only the FIRST error for each line.

Uncorrected errors

Some of the errors in the output file you may choose to ignore. For example, you may be using an input file created from another source system (such as 8920 Network Traffic Management software) and only a subset of the records in it are valid for NTP.

Error file example

Let us say, to insert three records into the domain table, you made the following ASCII input file named temp:

```
#domi;description;st;vpnbound
new1;This is the first;typex;y
new2;This is the second;typex;y
new3;This is the third;typex;y
```

Then you entered the following (note that it contains "-l 1", which means stop processing if one record fails — you would NOT normally set such a low error limit):

`dbedit  -i -t  domain -f temp -l 1 -s";"`

A screen message says:

```
*** 2 lines processed ***
    1 comment line
    0 records inserted
    1 record rejected due to an error

*** 2 lines not processed ***
dbedit completed with errors.  Errors saved in file
 domain.error
```

So, the error file, domain.error, contains:

```
#invalid value for field "domi": values for this field should
 not be longer than 3 characters

new1;This is the first;typex;y

# *** The following lines have not been processed

new2;This is the second;typex;y

new3;This is the third;typex;y
```

Why records are rejected

This table shows some reasons why dbedit rejects records. Here the domain table is used as an example:

Reason	Example	
	The input file, temp, has header `#domi;description;st; vpnboun d;npt` **and this record**	**And, after you enter dbedit -i -t domain -f temp -s";" the domain.error file says:**
Invalid value for a field	*new1* ;*descriptive text* ;pots;y;*descriptive text*	`#invalid value for- field "domi": values for- this field should not be- longer than 3 characters`
	new ;*descriptive text* ;pots;y;*descriptive text*	`#invalid value for- field "domi": must be a v- alid whole number`
Bad syntax, such as missing delimiters	`111` *descriptive text* `pots y` *descriptive text*	#Not all of the necessary fields have been specified.
Database dependencies (see "Field Dependencies" (p. 3-38)).	111;*descriptive text* ;*xxx* ;y;*descriptive text*	`#invalid value for- field "st": must be a valid entry for the "type- " field of the St table`

Correct dbedit errors

Procedure

Use this procedure to correct errors detected in the input file resulting from dbedit.

1 Use a text editor (such as **vi**) to go into the error file and make corrections according to error messages in the file.

Example: You previously created a file with:
dbedit -i -t domain -f temp -s";" A screen output message says, for example:

```
*** 4 lines processed ***

    1 comment line

    0 records inserted

    3 records rejected due to errors

dbedit completed with errors.  Errors saved in file
 domain.error
```

The error file in this example is `domain.error`

2 Rename the error file.

Example: If the error file is named domain.error, enter
mv domain.error domain1

- If the error file is named domain1.error, enter **mv domain1.error domain2**

You must do this if you used the default (instead of -o option) name for the error file. Otherwise, in the next step, if you enter, for example:
dbedit -u -t domain -f domain.error -s";"

your**dbedit** will fail, with the message: "The input and output file names must be different.

3 Use **dbedit** on the corrected and renamed error file.

Example: Enter **`dbedit -i -t domain1 -f temp -l 25 -s";"`**

4 Did you receive a message saying "Errors saved in file..."

- If no, you are done. (You should remove the unwanted error files and the temp file.)
- If yes, go back to *Step 1* and correct more errors.

END OF STEPS

dbedit Insert or Update Example

Example: Dbedit to insert or update

This is an example of using dbedit to insert (add) or update records to a database.

1 Use **`sui find`** to make a backup ASCII file of the table you are going to alter.

Example: If you are altering the domain table, enter

```
sui find source=domain noheader delim='";"' > hold_domain
```

2 Look up the table to be modified by using the describe command (see "describe Command" (p. 3-10)).

3 From the table description, make a note of:

- Each field's size and type (string, digit, set value, date-time)
- Which fields are key fields.
- Field dependencies.

Example:

- Domain has four fields: domi (3-digit), description (40-character string), st (5-character string), and vpnbound (set value, y or n).
- The domi field is key.
- The st field is dependent (a value used in this field must be in the type field of the st table).

For records to be inserted, you can now verify that the key field (or fields) for each record you are inserting is NOT already used. For example, if you plan to insert a record with key field (domi) of 91, enter

```
sui find source=domain search=domi=91
```

If this shows that a record already exists with domi of 91, then do not bother inserting it. If you do attempt to insert it, dbedit will give you an error messages telling you the insert failed (Step 8).

4 Use **`sui find`** to copy the header and first record from the database into a temp file.

For domain, enter

```
sui find source=domain noheader delim='";"' maxsave=1 > temp
```

Important! If you are doing updates, you can **`sui find`** the records to be updated from the database into the temp file and edit those records, instead of typing them from scratch.

5 Use a text editor (such as **vi**) to open the temp file.

Example: For domain, you would now see a header record and one record, resembling this:

```
#Domi;Description;St;Vpnbound

81;-;pots;n

~

~

~

"temp" 2 lines, 42 characters
```

The header record is harmless, since it starts with "#". The first record after the header is for your reference. Before you finish with the file you must either overwrite it with the new record, delete it, or insert a # as its first character.

Reference: For how to use **vi** , see "Edit (vi) ASCII Files" (p. 3-13) .

6 Enter each new record in the file, and save the file.

Important!

- Use semi-colons (;) to separate fields.
- Follow what you noted in *Step 3* .

7 Use **dbedit** with the **-i** (insert only), **-u** (update only), or **-iu** (insert or update) option.

Example: To add records from a file named temp to the domain database, enter
dbedit -i -t domain -f temp -s";"

Result: For large input files, after every 1,000 records, you see:
`***1000 lines processed***`

A successful completion looks like this:

```
***8 lines processed***

   5 records inserted

   3 records updated

dbedit completed successfully.
```

8 Did you receive a messages ending with: "Errors saved in file..."?

- If no, go to the next step.
- If yes, see “Correct dbedit errors” (p. 3-30) .

9 Use **`sui find`** to check your changes.

Reference: See “sui find for dbedit” (p. B-20) .

10 Remove the temp file.

Important! Save the backup (from *Step 1*), for a few days at least, or until you are sure you caused no harm.

END OF STEPS

dbedit Delete Example

Example: Dbedit to delete

This is an example of using dbedit to delete records to a database.

1 Make a backup ASCII file of the table you are going to alter.

Example: If you are altering the domain table, enter

```
sui find source=domain noheader delim='";"' > hold_domain
```

2 Look up the table using the describe command ("describe Command" (p. 3-10)).

3 From the table description, make a note of which fields are key fields.

Important! Something else you care about is what fields in OTHER tables are dependent on values in fields in to-be-deleted records. Although you could check this yourself (see "Field Dependencies" (p. 3-38)), it is easier to let the dbedit command find these dependencies, in which case the delete fails for the depended upon records. (In some cases, such a delete may not fail, requiring later cleanup. See "Verify Reference Database Tables" (p. 3-48).

Example: The domi field is the key of the domain table.

4 Create a temp file holding a copy of each record to be deleted. To do this you can either:

- Use **vi** to create such a file (If you do this, remember that you need only the key fields, but include semi-colons for omitted fields. For example, to delete Domain 91, in the temp file enter **91**.)
- Use **sui find** to copy the to-be-deleted records from a database into a temp file.

5 Use **dbedit** with the **-d** (delete option).

Example: To delete records in a file named temp from the domain database, enter

```
dbedit  -d -t  domain -f temp -s";"
```

6 If you receive a message ending with:

- "dbedit completed successfully", go the next step.
- "Errors saved in file...", see "Correct dbedit errors" (p. 3-30).

7 Use **`sui find`** to check your changes.

Reference: See "sui find for dbedit" (p. B-20).

8 Remove the temp file. Enter **`rm temp`**

Important! As a precaution, save the backup (from *Step 1*) for a few days.

END OF STEPS

Create Working Versions of Converter Files in $USERDIR

Purpose

All product provided converter files, such as fetcher configurations (**.cfg** files), filters, and fetchers, are delivered in the **$MODELDIR** directory. The product can change these files in every release, and an upgrade is not expected to save or preserve those changes.

Customers specific changes reside in **$USERDIR**.

If 8920 NTP does not find the customized converter files in **$USERDIR**, it will use the files supplied with the product from **$MODELDIR**.

Procedure

Use the following procedure to create working versions of converter files in **$USERDIR**:

1 Create a directory **$USERDIR/fetchers_cfg**

2 Copy the **$MODELDIR/** <*type of files*> **_fetcher.cfg** template file to **$USERDIR/fetchers_cfg**

3 Use a text editor (such as **vi**) to change the file, as needed.

Additional information When populating the **fileconfig** reference table, add the following line to the **filefetcher** field:

-f $USERDIR/fetchers_cfg/ <*type of collector*> **_fetcher.cfg**

The complete contents of the **filefetcher** field should resemble this:

<*type of collector*> **_fetcher -f $USERDIR/fetchers_cfg/** <*type of collector*> **_fetcher.cfg -e $MODELDIR/** <*type of collector*> **_filter**

END OF STEPS

Filter files

Use the same procedure for <*type of collector*> **_filter** files. Note that the complete contents of the **filefetcher** field should resemble this:

<*type of collector*> **_fetcher -f $USERDIR/fetchers_cfg/** <*type of collector*> **_fetcher.cfg -e $USERDIR/filters/** <*type of collector*> **_filter**

Field Dependencies

Field Dependency During Updates

Purpose

In some cases, before you can put a value in a field in one database table, that value must already be defined in a field in another database table. Otherwise, the dbedit or other command fails.

Similarly, before you delete a record in one table, you need to insure it is not used in another table.

Alphabetical list

This table is an alphabetical lists of reference database tables, with field dependencies.

In table...	Before you put a value in field...	That value must be found in field...	In table...
acode2fdc	fdc	fdc	fdc
adjarch	swclli	clli	swarch
	stp	ne	stparch
adjroute	adjclli	adjclli	adjarch
	signet	name	signet
alert_levels	alert_type	type	alertdef
alert_notify	notify_id	notify_id	notify
	tablename	tablename	menutables
alertdef	srcmodel	model	chron_info
alertfq	type	type	alertdef
alertperiods	type	type	alertdef
ccconfig	source	name	source
	conversion_name	conversion_name	bildtsrec (internal table)
cellroute	clli	re	rearch
	De	clli	swarch
city	ccd	ccd	country

In table...	Before you put a value in field...	That value must be found in field...	In table...
cmdgroupmap	cmdgroup	name	cmdgroup
	command	name	command
cos	st	type	st
country	npt	npt	npt
custid	custname	cust	customer
de2route	rt	rt	rtarch
	de (None, since de2route is for *4ESS* only, and *4ESS* CIMs give De)		
disabledig	fdc	fdc	fdc
dmsroute	clli	re	rearch
	de	clli	swarch
	sig	type	signaling
domain	st	type	st
	npt	npt	npt
ecosroute	re	re	rearch
	area	area	ecosarch
ess1a2fdc	fdc	fdc	fdc
	sig	type	signaling
ewsdroute	clli	re	rearch
	de	clli	swarch
fdc	sig	type	signaling
	st	type	st
fdc2tn	fdc1-fdc7	fdc	fdc
fdcgroupmap	fdcgroup	name	fdcgroup
	fdc	fdc	fdc
fdcpermit	fdcgroup	name	fdcgroup
fileconfig	source	source	ccconfig
gtspec	st	type	st
homedigits	cic	cic	carrier
	ccd	ccd	country
id2ne	ne	clli	swarch
intcpdial	source	name	source

In table...	Before you put a value in field...	That value must be found in field...	In table...
iparch	owner	id	owner
ixcarrier	cic	cic	carrier
lrarch	clli	clli	swarch
lrn2ne	ne	clli	swarch
		scpclli	scparch
		ne	stparch
		adjclli	adjarch
		area	ecosarch
lspcalendar	datype	datype	lspdays
lsphours	datype	datype	lspdays
man_thresh_xx	lspid	each unique pairing of values in the daytype and lspid fields, such as b0, b1, b2...w0, w1, w2...	lsphours
	FQ fields	Use describe command to view FQ fields.	
mean_xx	lspid	each unique pairing of values in the daytype and lspid fields, such as b0, b1, b2...w0, w1, w2...	lsphours
	FQ fields	Use describe command to view FQ fields.	
mt20route	clli	re	rearch
	de	clli	swarch
netgroupmap	netseg	name	netseg
netpermit	sysuser	login	sysuser
	netseg	name	netseg or netgroup
netsegmap	netseg	name	netseg
	ne	clli, scparch, ne, adjclli, or area	swarch, scparch, stparch, adjarch, or arch
notify	sysuser	login	sysuser
oline2st	st	type	st
otr2fdc	fdc	fdc	fdc

In table...	Before you put a value in field...	That value must be found in field...	In table...
outtcpdial	source	name	source
pc2clli	clli	clli	swarch
potsroute	ne	clli	swarch
pptemp_ columns	template_name	template_name	pptemplate
	tablename	tablename	menutables
pptemplate	tablename	tablename	menutables
rearch	re	clli, ne, rt, area, or adjclli	swarch, stparch, lrarch, rtarch, ecosarch, or adjarch
	source	name	source
referral	ne	clli, scpclli, ne, adjclli, or area	swarch, scparch, stparch, adjarch, or ecosarch
	fdc	fdc	fdc
reports	fdcgroup	name	fdcgroup
rearch	re	clli	swarch
	source	name	source
roaming	None		
route1a	clli	re	rearch
	de	clli	swarch
route5e	clli	re	rearch
	de	clli	swarch
s1240route	clli	re	rearch
	de	clli	swarch
samplingrate	re	re	rearch
	fdc	fdc	fdc
scode2sig	signaling	type	signaling
	ne		
scparch	stp	ne	stparch
scproute	scpclli	scpclli	scparch
	signet	name	signet

In table...	Before you put a value in field...	That value must be found in field...	In table...
sdthresh	fdc	fdc	fdc
	ne	clli, scpclli, ne, adjclli, or area	swarch, scparch, stparch, adjarch, or ecosarch
searchalias	ne	clli, scpclli, adjclli, or area	swarch, scparch, adjarch, or ecosarch
source	name	name	bdrhost
stcode2st	st	type	st
stparch	owner	id	owner
	signet	name	signet
swarch	cc	cc	country
	eqtype	type	eqtype
	stp	ne	stparch
	owner	id	owner
sysuser	cmdgroup	name	cmdgroup
	fdcgroup	name	fdcgroup
univconfig	source	name	source
univroute	clli	re	rearch
	de	clli	swarch
	sig	type	signaling
vpnid	custname	cust	customer
vpnroute	signet	name	signet
	scpclli	scpclli	scparch

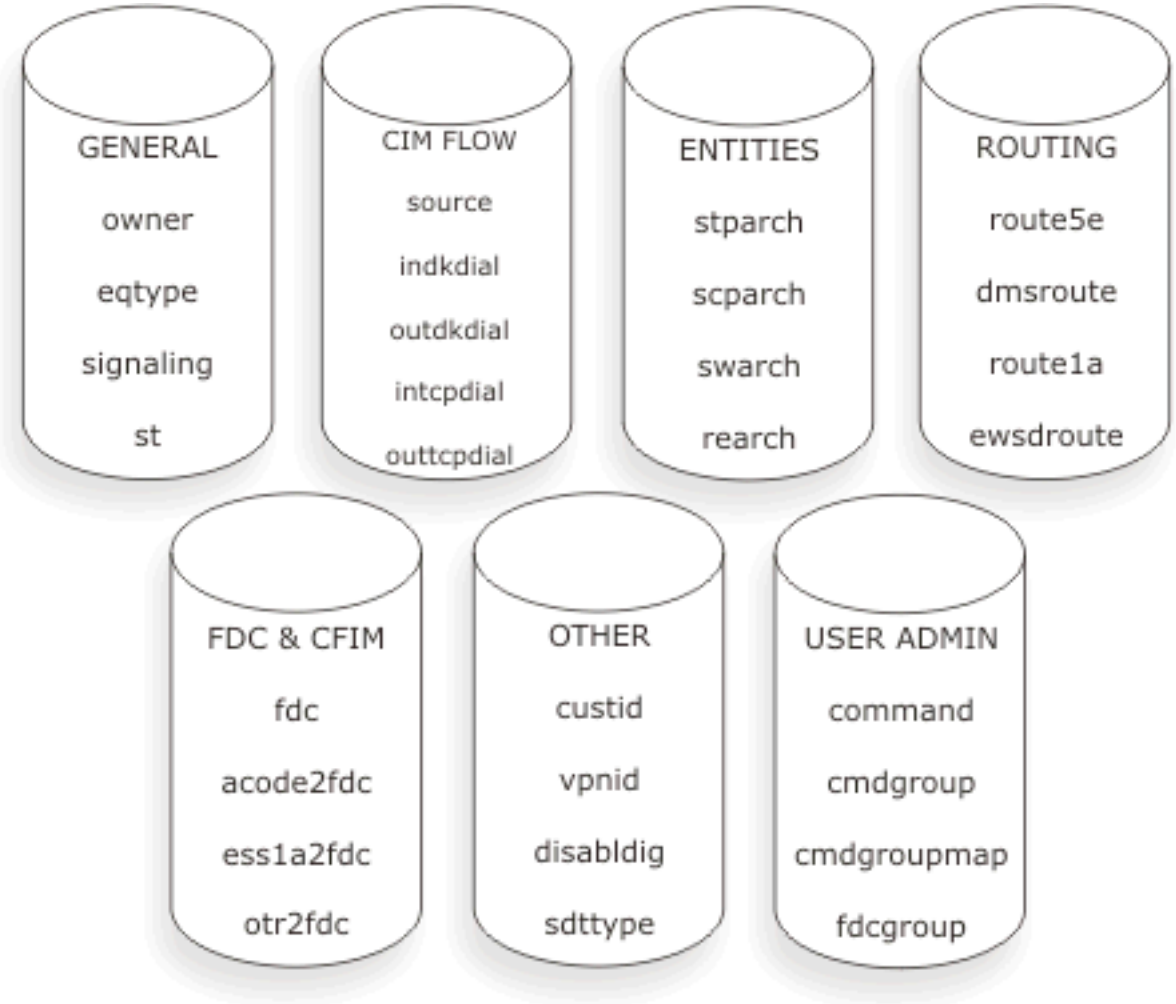
Field Dependency During Installation

Purpose

Often, before you can put a value in a field in one database table, that value must already be defined in a field in another table. Otherwise, the dbedit or other command fails. During installation, the best way to avoid field dependency problems is to install tables in a specific order. Most often, you use dbedit to install values in a table, or update values preloaded in the table. But some tables use other tools (for example, the add_ntpuser command adds a record for a NTP user to the sysuser table).

Installation order summary

This illustration summarizes information in the table at "Installation order" (p. 3-44). For complete information, see that table.



Installation order notes

The list "Installation order" (p. 3-44) gives installation order. Columns are as follows:

Column	Description
Group	Install tables in each group before installing the next group.
Install...	Indentions (" — ") mean you first install the table indented from (above the indented table). If no indentions are shown the order shown is recommended but not required.
After...	This shows the order of tables.
Pre-populated	During installation, values are either: • *Y* —Preinstalled. Your NTP support organization can help you modify them. • *N* — NOT preinstalled. Your NTP support organization can help enter values you provide.

Installation order

To avoid failure by dbedit, sysuser, or other commands affecting databases, install tables in the order given in this table.

Important! Your system may not use all tables listed.

Group	Install...	After...	Prepopulated
General	owner	None	N
	rqtype	None	Y
	signaling	None	Y
	st	None	Y
	— gtspec	st	Y
	— domain	st, npt	Y
	fcause	None	Y
	menutables	None	Y
	samplingrate		Y
	signet	None	Y
	bdrhost	None	N
CIM flow	npt	None	Y
	source	bdrhost (only if you use RDS — refsynch)	N

Group	Install...	After...	Prepopulated
	— indkdial	source	N
	— outdkdial	source	N
	— intcpdial	source	N
	— outtcpdial	source	N
	collectors	None	Y
	— bildscoll	collectors	Y
Entities	lrarch	None	N
	stparch	owner, signet	N
	— scparch	stparch	N
	— swarch	rqtype, stparch, owner	N
	— — rearch	source, swarch	N
	— — adjarch	swarch, stparch	N
	— — pc2clli	swarch	N
	ecosarch	None	N
	rtarch	None	N
	route5e	rearch, swarch	N
Routing	dmsroute	rearch, swarch, signaling	N
	scproute	scparch, signet	N
	route1a	rearch, swarch	N
	ewsdroute	rearch, swarch	N
	s1240route	rearch, swarch	N
	ecosroute	rearch, swarch	N
	adjroute	adjarch, signet	N
	de2route	rtarch	N
	cellroute	swarch, rearch	N
	hlrroute	lrarch, rearch	N
	potsroute	swarch	N
	vpnroute	scparch, signet	N
	vnivroute	rearch, swarch, signaling	N
FDC & CFIM	fdc	eqtype, signaling, st	Y

Group	Install...	After...	Prepopulated
— acode2fdc	fdc	Y	
	— ess1a2fdc	fdc, signaling	Y
	— otr2fdc	fdc	Y
	— fdc2tn	fdc	Y
	lrn2ne	swarch, scparch, stparch, adjarch	N
	oline2st	st	N
	dcode2d	None	Y
	scode2sig	signalling	Y
	stcode2st	st	Y
	id2ne	swarch	Y
Other	carrier	None	Y
	city	country	Y
	custcode	None	N
	custid	None	N
	custip	None	N
	customer	None	N
	vpnid	None	N
	disabledig	fdc	N
	ixcarrier	carrier	N
	latacode	None	N
	lspcalendar	lspdays	N
	lspdays	None	Y
	lsphours	lspdays	Y
	man_thresh_xx	lsphours	Y
	mean_xx	— lsphours — man_thresh_xx	Y
	sdttype	None	?
	cos	st	N
	referral	fdc; swarch, scparch, stparch, adjarch, ecosarch	N
	searchalias	swarch, scparch, adjarch, ecosarch	N

Group	Install...	After...	Prepopulated
	sdthresh	fdc; swarch, scparch, stparch, adjarch, ecosarch	N
	country	npt	Y
User admin	command	None	Y
	cmdgroup	None	N
	— cmdgroupmap	command, cmdgroup	N
	fdcgroup	None	N
	— fdcgroupmap	fdc, fdcgroup	N
	— fdcpermit	fdcgoup	N
	netseg	None	N
	— netsegmap	netseg, (any) swarch, scparch, stparch, adjarch, ecosarch	N
	netgroup	None	N
	— netgroupmap	netgroup	N
	— netpermit	sysuser, (either) netseg or netgroup	N
	— reports	fdcgroup	N
sysuser	cmdgroup, fdcgroup, netgroup	N	
notify	sysuser	N	
Pattern painter	pptemplate	None	Y
	— pptemp_columns	pptemplate	Y

Verify Reference Database Tables

Database Schema

Overview

The data in database tables is checked three ways:

- Dbedit. During execution of the dbedit command, with errors sent to a file. See "Correct dbedit Errors" (p. 3-27).
- Audits. If dbedit failed to prevent a problem, you may need to run an audit. See "Application Audits" (p. 3-49).
- Incon logs. The incon logs record inconsistencies, such as incoming data that cannot be converted due to inconsistencies in database definitions (missing or logically incompatible definitions). See incon logs on "incon Log" (p. 10-29).

Application Audits

Purpose

The audit command checks for inconsistencies in the following reference database tables:

Audit this table	To verify that É
adjarch	• Adjunct frames (NSCX and Conversant only) identified in this database table are also identified in the adjroute database table.
digits (multi-table)	• There are no duplicate digits across the ADJROUTE, SCPROUTE, POTSROUTE, and VPNROUTE tables. (The same digit in two or more tables is a duplicate.) • There are no duplicate DIGITS field between the CUSTID and VPNID tables.
dmsroute	• Every CLLI code in dmsroute corresponds to an RE in the rearch table whose conv field is DMS.
ewsdroute	• Each CLLI in the EWSDROUTE table is also an RE with CONV='ewsd' in the REARCH table.
fdc	• For every FDC with swtype equal to *4ESS* there is at least one Sampling Rate record in the sampling rate database table. • For each FDC there is at least one fdcgroupmap record.
netsegmap	• Each network entity (also known as network element) in the adjarch, ncparch, separch, and swarch tables is assigned to at least one netseg in the netsegmap table.
owner	• Only one ID has its type equal to "owner".

Audit this table	To verify that É
rearch	• All switches with conv equal to 5ess have at least one entry as a CLLI code in the route5e table. • All switches with conv equal to DMS have at least one entry as a CLLI code in the dmsroute table. • All switches with conv equal to 1aess have at least one entry as a CLLI code in the route1a table. • All switches with conv equal to 4ess have at least one sampling rate record. • All switches with conv equal to ewsd have at least one entry as a CLLI in the ewsdroute table. • All switches with conv equal to s1240 have at least one entry as a CLLI in the s1240route table. • All records with a source whose type is equal to CP do not have "-" as the value of the tag field. • All combinations of source and tag are unique for sources whose type is equal to CP.
route1a	• Every CLLI code in the route1a table corresponds to an RE in the rearch table whose conv field is equal to 1aess.
route5e	• Every CLLI code in the route5e table corresponds to an RE in the rearch table whose conv field is equal to 5ess.
s1240route	• Each CLLI in the S1240ROUTE table is also an RE with CONV='s1240' in the REARCH table.
scparch	• Each SCP has one and only one mate. • Each pair of mates has the same STP.
sdthresh	• Each FDC is listed with a TM of "d" in the FDC table.
univroute	• Every CLLI code in the univroute table corresponds to an RE in the rearch table whose conv field is equal to univ. • Each CLLI in univroute table is also an RE with conv of "univ" or "gtds" in the rearch table.

Audit command

The audit command checks for inconsistencies in reference database tables. You run it from shell. Output is stored in an ASCII file, which you can print, vi, cat, or use as an input file to dbedit.

Syntax

The audit command has the following syntax:

audit [-t type] [-o output file]

Example: To audit the fdc table and send the output to the file fdcout, enter:

audit -t fdc -o fdcout

Parameters

-t type — The type parameter identifies the particular audit to be performed. Valid values are:

all (audits all of the other items in this list)

- adjarch
- digits
- dmsroute
- ewsdroute
- fdc
- netsegmap
- owner
- rearch
- route1a
- route5e
- univroute
- s1240route
- scparch
- sdthresh
- univroute

-o output file — Names the file where the output is to be stored. If this is omitted, the default file name is audit.out.

Output example

The following is an example of output of an audit of the fdcount file:

```
fdc's not in fdcgroupmap table
  444003
  444004
  444005
  444006
  444007
  444010
  444vca
  aufdc3a
  aufdc3b

fdc's not in swsampling table
  444000
  444001
  444002
  444003
  444004
  444005
  444006
  444007
  444008
  444009
  444010
  aufdc3b
```

Phone Audit Command

Overview

The phone_audit command is an optional feature used to determine whether provisioned phone numbers on a switch are actually producing usage records. This help network analysts determine which phone lines are not producing billing records.

The phone_audit command verifies that the ROPT_PHONE_AUDIT option is enabled before executing.

This command is executed daily at 2:00 a.m. from cron. It can also be run manually as needed.

phone_audit command

The phone_audit command is as follows:

```
phone_audit rolloff=<days> clli=<clli[,clli,clli]>
 daysback=<days>
```

Where:

- rolloff=<days> has a default of 60 days. Any records with a usage date older than <days> are removed before any auditing is done.
- clli=<clli[,clli,clli]> has a default of all cllis
- daysback=<days> has a default of 1 day

Viewing Output

Output from the phone_audit command is viewed on the GUI by accessing the Recent Change Audit Report. This report provides information about recent changes such as phone number, change date, and the number of days with no billing record since the phone number was activated.

For more information about the Recent Change Audit Report, see Chapter 7, "Reports", in the *BB-GUI User's Guide*.

Trunk Group Usage Audit

Overview

The Trunk Group Usage audit is an optional feature that allows you to determine whether trunk groups on a switch are properly recording usage records. This helps network analysts find trunk groups that are incorrectly provisioned and not producing billing records.

Using the tg_usage table (see “tst_num_std_rule” (p. A-161)), NTP processes nightly records from trunk groups. It sums data from the associated CFIMs. If there is a discrepancy between that summed number and the total minutes of usage, it will show as a difference in the CDRMOU and TGNMOU fields.

Viewing Output

Output from the Trunk Group Usage audit is viewed on the GUI by accessing the Trunk Group Audit Report. This report provides information such as trunk group number, number of billing records, minutes of use, holding time, and billing record usage

For more information about the Trunk Group Audit Report, see Chapter 7, "Reports", in the *BB-GUI User's Guide*.

4 Add Network Elements

Overview

Purpose

This chapter is about administering Network Trouble Patterning software reference databases so network elements and network topology appropriately appear in the CFIM fields.

Contents

Introduction

Introduction To Network Elements

Purpose

This chapter is about administering NTP reference databases so network elements and network topology appear in the following CFIM fields.

CFIM field	Definition	Reference
RE	Reporting entity. The entity sends CIMs (call information messages) to NTP. These messages may represent either unsuccessful or successful events.	"RE and DE description" (p. 4-6)
DE	Distant entity. An element referenced in the CIM, such as a switch an RE failed to reach or successfully connected to.	
Related	Related entity. A related entity is a network element that is part of setting up a call. Among different conversions (see "What is a "conversion"?" (p. 4-10)), there is much variability about how and whether the Related field is populated.	"Diagram 2" (p. 1-29)
Rs, Ds	Reporting and distant STPs and the mapping to REs defined in the swarch table.	"stparch Table" (p. A-155)
Rt	Appears on CFIMs from the 4ESS conversions only.	"Rt illustration" (p. 4-50)
Sfx (optional)	Appears on CFIMs from the 5ESS(MDII), DMS, *Sonus*, EWSD, and GTD5 conversions only.	"Trunk Group Suffix (Sfx)" (p. 4-58)

Note

Please note that:

- Other CFIM fields are network elements, but are NOT covered in this chapter because they require little administration—either because they are taken directly from CIMs or use a simple code-to-output conversion from pre-filled administration tables.
- Fields above are thresholded as follows:
  - RE — RE/FDC
  - DE — DE/FDC

Add and delete

Important!

- **`Add`**. Various procedures in this chapter tell how to add network elements.
- **`Delete`**. To delete an element, use its "Add" procedure, but in reverse order. See "OTR fields you can affect" (p. 4-91) for tips and guidelines.

Dbedit

This chapter uses **`dbedit`**. Note the following:

- For how to use **`dbedit`** for addition, modification, and deletion of database records, see "dbedit Insert or Update Example" (p. 3-32).
- For what values to assign to each field in a table, see each table in, Appendix A, "Reference Database Tables".
- We urge you to back up each table into an ASCII file before you **`dbedit`** it. For example, to back up the swarch table, enter

  ```
  sui find source=swarch noheader delim=' ";" ' > swarch.backup
  ```
- Several procedures ask you to **`sui find`** a record from a file and use it as a template, or sample file, to modify and use for database modifications. For example to get a template from the rearch table, enter:

  ```
  sui find source=rearch noheader delim=' ";" ' maxsave=1 > temp
  ```

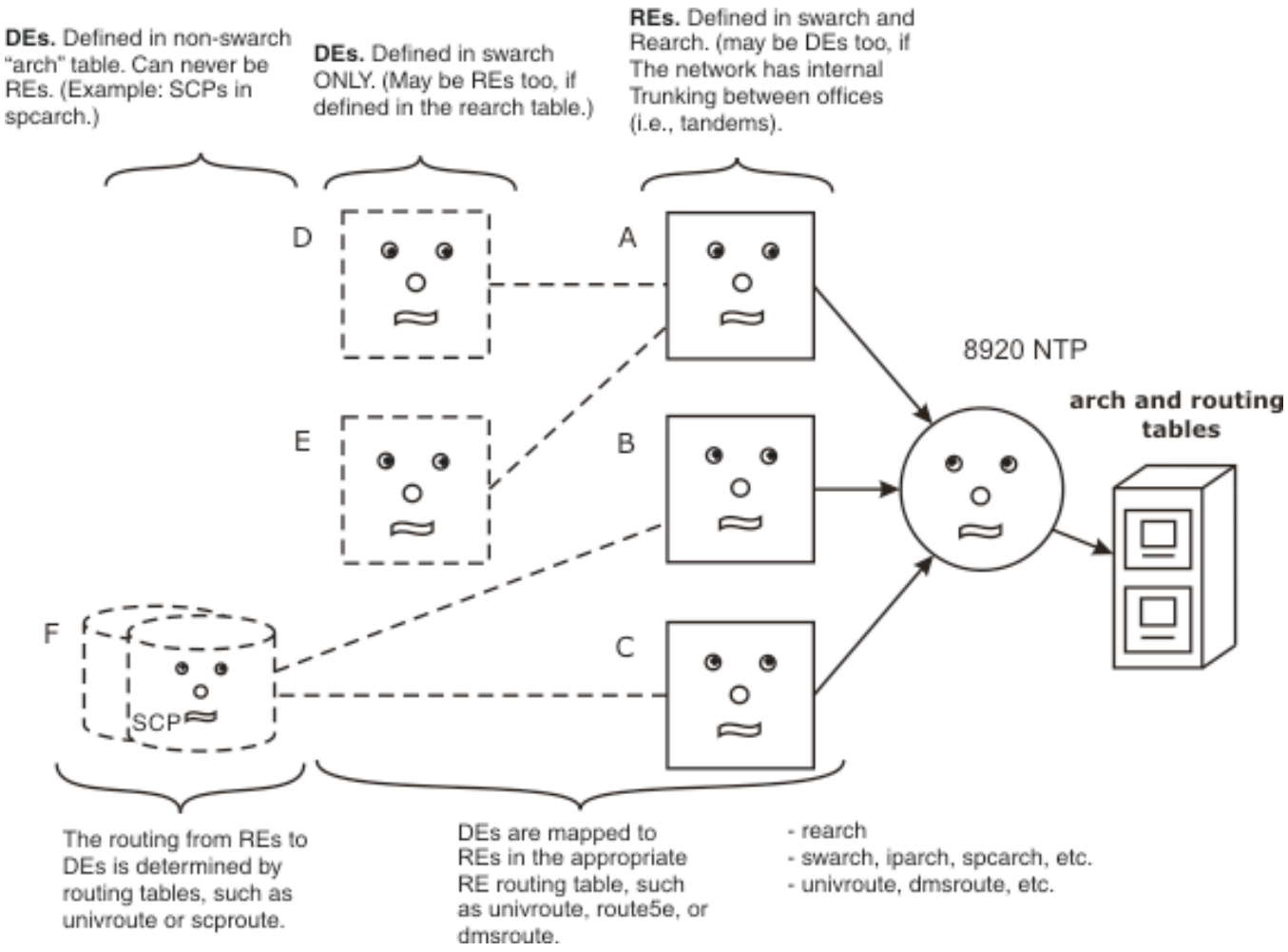
  If you do this, and the temp file is empty, it means there are currently no records in the database. If that happens, you must create the record with a text editor (such as **`vi`**), without a template.

RE and DE

RE and DE Overview

RE and DE description

NTP sees REs and DEs according to what you put in NTP's routing and architecture tables.



In this illustration:

- **RE**. A, B, and C are REs.
- **DE**.
  - A sees B, D, and E as DEs (per their route tables).
  - B sees A as a DE (per its route table).
  - B and C see F as a DE (per their scproute table).

"Arch" and route tables

This section shows:

- "Arch" tables where REs and DEs are defined.
- Routing tables where REs are mapped to DEs. (For more information [by conversion], see "Map an RE to its swarch DEs" (p. 4-68).)

A network element in this CFIM field	Is defined in this "arch" table	REs are mapped to DEs in this route table	Reference
RE	swarch, then rearch	Each RE's own routing table (Example: If RE/DE is a 5ESS, use the route5e table)	"Add an RE" (p. 4-17)
DE, where the DE could also be an RE	swarch	Remember, an RE can be DE to another RE, if mapped in the other RE's routing table.	"Map an RE to its swarch DEs" (p. 4-68)

A network element in this CFIM field	Is defined in this "arch" table	REs are mapped to DEs in this route table	Reference
DE, where the DE could never be an RE	DE's own "arch" table (except cell base stations)	DE's own routing table (except location registers)	"Add DE-Only Elements" (p. 4-31)
• SCP	• scparch	scproute Also defines Rs and Ds fields on CFIMs.	• "Add an SCP as DE" (p. 4-34)
• Cell base station • Location register	• swarch There is no "loca-tion register route" table. • lrarch	• cellroute Maps to AUTOPLEX (5ESS) or DMS MTX MSC/DMS MSC RE's to cells. • To map to: • AUTOPLEX MSC RE's, use route5e • DMS-MTX MSC and DMS MSC RE's, use dmsroute There is no cellarch. Instead use swarch, with eqtype of base or cell. (Unlike other values in swarch, cell base stations can NOT be put in Rearch to become RE's.)	• "Add a cell base station" (p. 4-42) • "Add a location register as a DE" (p. 4-38)
• ECOS area Supported by 4ESS network elements.	• ecosa-rea	• ecosroute	• "Add an ECOS area as DE" (p. 4-47)

A network element in this CFIM field	Is defined in this "arch" table	REs are mapped to DEs in this route table	Reference
• Adjunct	• adjarch	• adjroute	• “Add an adjunct as DE” (p. 4-44)

RE Conversions

What is a "conversion"?

How you administer network elements depends on how NTP converts CIMs to CFIMs for a specific implementation. A "conversion" means whatever NTP does to an RE's CIMs to CFIMs.

This term refers not just to the message parser NTP uses in CIM-to-CFIM conversion, but also to the administrative procedures used to set up the interface between the RE and NTP. There are different conversions for different, combination of RE type and sources type.

Reference: Conversions are listed in the second column of the table at "Recognize a CFIM's conversion by Retype on CFIM" (p. 4-12)).

Why discuss conversion?

You need to be aware of conversions in two cases:

- *Troubleshoot CFIMs*. If something is wrong with a CFIM, you need to know its conversion, to know what tables and fields to check. See "Find a CFIM's conversion" (p. 4-11).
- *Add REs*. Before you can add an RE, you need to know its conversion to know what tables and fields to populate. See "Figure out what conversion to use" (p. 4-16).

Conversion examples

For example, adding a 5ESS RE differs according to which of the following conversions NTP will use.

- 5ESS conversion — used if RE's source is an NFM (or other EMS).
- GeoProbe conversion — used if the RE's source is a GeoProbe.
- IPDR conversion — used if the RE's CIMs are IPDRs, regardless of source.
- 7R/E Direct TCP/IP conversion — Used if we collect CIMs from a 5ESS ASM (administrative services module).

Find a CFIM's conversion

Procedure

Important! You may be able to spot a CFIM's conversion by the following:

"Recognize a CFIM's conversion by Retype on CFIM" (p. 4-12).

"Recognize a CFIM's conversion by Source on CFIM" (p. 4-14).

Use this procedure to find out what conversion a CFIM's RE uses, and to then find out what fields and tables to check to fix CFIM problems.

1 Look up a CFIM's RE in Rearch, and then look in the record's Conv field for the conversion.

Important! You may also need to see the Source table.

2 If the CFIM is from a consultant-added CDR conversion, see your Alcatel-Lucent consultant for tables and fields used. Otherwise, for:

- What tables a conversion uses, see "Tables to dbedit to add an RE" (p. 4-25).

END OF STEPS

Recognize a CFIM's conversion by Retype on CFIM

If you know you have implemented only some conversions, and they do not overlap (do not put the same values in Retype), you can use this table alone to recognize a CFIMs' conversions. (But see, "How Retype can be wrong" (p. 4-13).) If you need to be sure, use the procedure "Find a CFIM's conversion" (p. 4-11).

- These Retypes are what we recommend, but by adding values to the eqtype table, and using them in the Eqtype field of the swarch table, the system administrator can cause virtually anything to appear in a CFIM's Retype (or Detype) field.
- OSPS, TOPS. For messages types collected, and feature numbers, see "DMS MSC FDCs" (p. 4-89).
- The following use the configurable converter (ccc): AXE 10, AXE 10 TRADO, Lucent Softswitch, IPDRs, and any from a consultant-added CDR conversion.

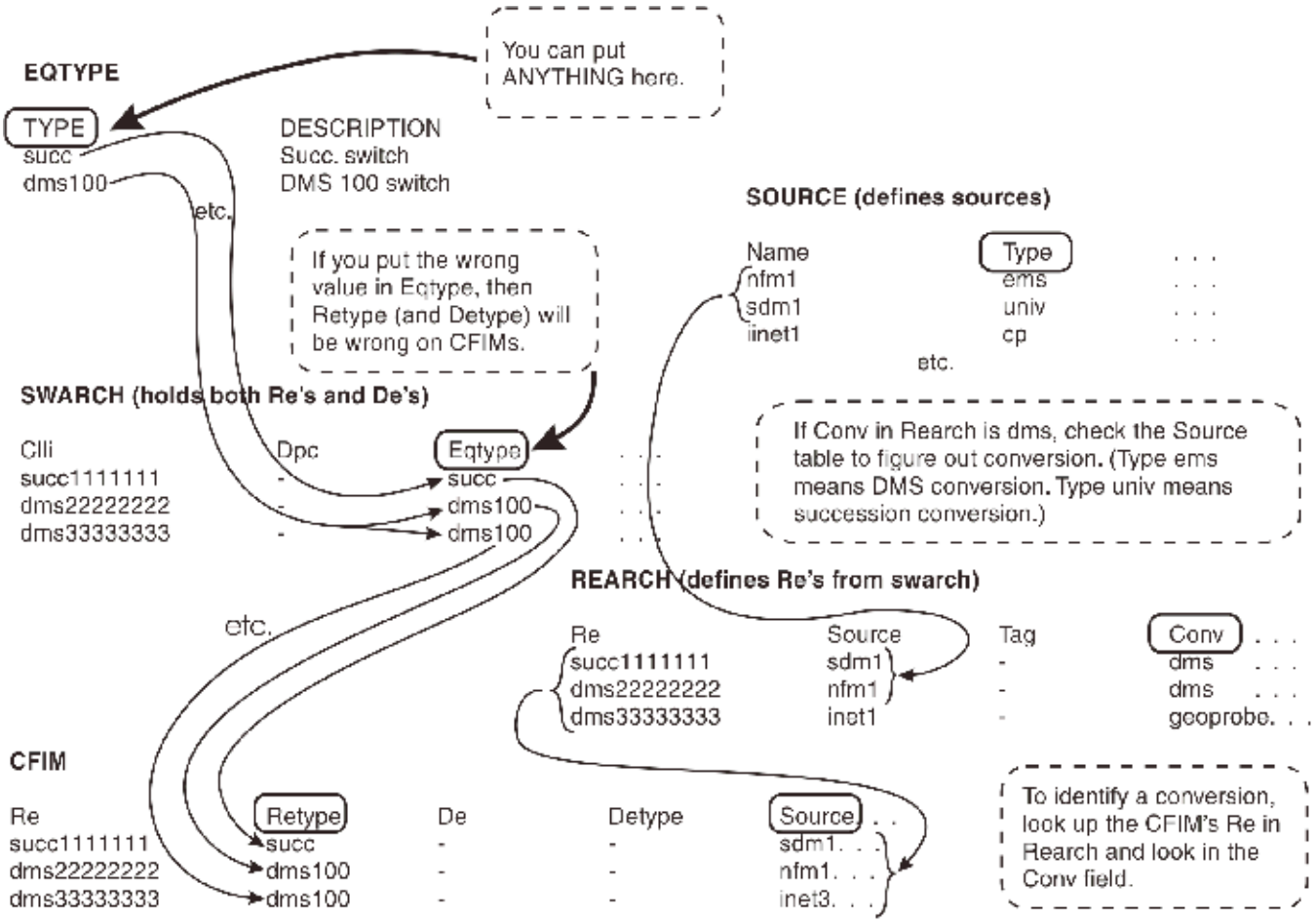
If you see this in a CFIM's Retype field	The CFIM probably came from this conversion
1aess	1AESS
4ess	4ESS
5ess	5ESS
7re_pds	7R/E PLS
autoplex (or 5ess)	AUTOPLEX MSC
dms-mtx (or dms)	DMS MTX MSC
nrtl-gsm	DMS MSC (Global System for Mobile Communications)
osps tops	OTR (5ESS OSPS module) OTR (DMS TOPS module)
dms100, dms200, dms250, or dms500	DMS
ewsd	EWSD
s1240	Alcatel S1240
succ	Succession SN05 and SN06
ANY monitored by a GeoProbe. Look in the Source field for a value (such as inet1) indicating a GeoProbe source.	GeoProbe
axe10 in the Retype field. (See the Source field, where there is a BILLDATS type sources, and an EMS or direct-from-switch source.)	AXE 10 AXE 10 TRADO
softsw	Lucent Softswitch

If you see this in a CFIM's Retype field	The CFIM probably came from this conversion
ANY monitored by a mediation system producing IPDRs. Look in the Source field for a value indicating an IPDR type source (such as navis1).	IPDRs
ANY, depending on the feature.	Any from a consultant-added CDR conversion.

How Retype can be wrong

You cannot be sure the Retype on CFIMs will identify the conversion. This is because the Retype field takes its value from the type field in the Eqtype table, and you can put ANYTHING in that field. If you put the wrong value in Eqtype, then Retype (and Detype) will be wrong in CFIMs.

Important! A conversion is really identified in the Rearch table's Conv field. (You may need to see the source table too — currently, you need do this only when the value in the Conv field is dms or dms-msc.)



You might think you can take a CFIM's FDC, look it up in the FDC table, and identify the CFIM's Retype in the FDC's Eqtype field. That may work, but a FDC's Eqtype can also be wrong.

Recognize a CFIM's conversion by Source on CFIM

The CFIM's Source field may indicate what conversion the CFIM used, if all three of the following are true.

- The name is meaningful (not just machine1, machine2, etc.)
- The name does NOT indicate an EMS (such as NFM1) or BILLDATS (such as billdats1), since those are not unique to one conversion.
- You know something about sources, as explained in this table.

If this does not help, use "Find a CFIM's conversion" (p. 4-11).

If the CFIM's Source field indicates this	The CFIM is probably from this conversion
NA since an EMS that is not unique to one conversion.	1AESS
A CP	4ESS
NA since an EMS is not unique to one conversion.	5ESS
NA (possibly OneLine Manager, such as olm1, olm2, etc.)	7R/E PLS
NA since an EMS	AUTOPLEX MSC
NA since an EMS	DMS MTX MSC
An OSPS	OTR (5ESS OSPS module)
A TOPS	OTR (DMS TOPS module)
NA since an EMS is not unique to one conversion.	DMS
NA since an EMS is not unique to one conversion.	EWSD or Alcatel S1240
An SDM	Succession SN05 and SN06
An INET Geoprobe	GeoProbe
NA since a BILLDATS	AXE 10
A TMOS	AXE 10 TRADO
NA since a BILLDATS is not unique to one conversion.	Possibly Lucent Softswitch
An IPDR-producing system, such as Navis	IPDRs
NA since the source could be anything.	Any from a consultant-added CDR conversion

Figure out what conversion to use

Purpose

Before you add an RE, you must determine what conversion it uses. Then you can use the procedure, "Add an RE" (p. 4-17). Note that:

- You may already know the appropriate conversion from adding previous REs. You can take a CFIM from an equivalent RE, and determine its conversion from "Find a CFIM's conversion" (p. 4-11).
- The CIM source may indicate the conversion type. For information on sources and conversions, see "Which source to use for an RE?" (p. 5-10).
- You can ask your NTP support organization for assistance.

Add an RE

Purpose

You should add STPs and SCPs first before adding other REs. See “Add and Map SCPs and STPs” (p. 4-32) .

Adding an RE is accomplished in several stages:

- “Procedure: Implement the Conversion” (p. 4-17)
- “Procedure: Make a Diagram” (p. 4-18)
- “Procedure: Add the RE to swarch” (p. 4-18)
- “Procedure: Get a Source” (p. 4-18)
- “Procedure: Add the RE to rearch” (p. 4-19)
- “Procedure: Add the RE's swarch-type DEs, and map the RE to those DEs” (p. 4-19)
- “Procedure: Add the new RE as DEs” (p. 4-20)
- “Procedure: Add the SCPs and map SCPs and STPs” (p. 4-20)
- “Procedure: Conversion Specifics” (p. 4-21)
- “Procedure: Test and Monitor” (p. 4-21)

Procedure: Implement the Conversion

1 Determine which conversion to use.

2 If this is the first RE to be added for a conversion, then you must first implement the conversion. With help from your NTP support organization:

1. Have the NTP support organization ensure the conversion is turned on (at installation time).
2. Make sure the source for this RE has been added to NTP.
3. See “Tables to dbedit to add an RE” (p. 4-25) ". Look at the column for the conversion, and ensure tables marked with "1" are populated with needed values. (Many such tables are pre-populated with values for all features.)

   Important! Some "1" tables are for defining FDCs, explained at “Add or modify an FDC” (p. 4-78) .

3 Continue with the next procedure.

END OF STEPS

Procedure: Make a Diagram

1 For reference throughout this procedure, draw a diagram showing the RE, its source, and NTP.

2 With help from the RE's administrator, draw in other elements the RE is connected to (such as SCPs, STPs, and possible DEs), and existing REs that see the new RE as a DE.

3 Continue with the next procedure.

END OF STEPS

Procedure: Add the RE to swarch

1 If the RE is not already in swarch, use "Add to Swarch (or other "arch") Table" (p. 4-61) to add the RE to swarch.

Important! The last step of that procedure is to use "Manage Network Groups and Segments" (p. 7-30) to add the network element to network groups or segments, as desired.

2 Continue with the next procedure.

END OF STEPS

Procedure: Get a Source

1 Determine the new RE's source (you will need it, for the Source field of the rearch table, in "Procedure: Add the RE to rearch" (p. 4-19)).

Important! You may be able to use an existing source, or you may need to add a new source. A few conversions require a new source for each RE. See Chapter 5, "CIM Source Administration" for what to do. To list sources in NTP, enter:

```
sui find source=source
```

2 Ensure the NTP interface to the source is activated. If source has an interface to more than one RE, it will probably already be active. Use "Activate or Deactivate a Source Link" (p. 5-17) .

3 Continue with the next procedure.

END OF STEPS

Procedure: Add the RE to rearch

1 Use "Add an entity to rearch" (p. 4-64) to add the new RE to rearch.

- If this is an Autoplex MSC conversion, continue with Step 2.
- If this is a GeoProbe conversion, continue with Step 3.
- Otherwise, STOP, you are done with this procedure. Continue with the next procedure.

2 If this is an Autoplex MSC conversion, add the ECP as RE. Then use this procedure again to add each 5ESS module as an RE. See "Tables to Edit to Add an RE" (p. 4-25) .

3 If this is a GeoProbe conversion and if a GeoProbe RE is already in rearch (for another conversion), add it a second time — with a GeoProbe in the Source field and univ in the Conv field.

4 Continue with the next procedure.

END OF STEPS

Procedure: Add the RE's swarch-type DEs, and map the RE to those DEs

1 Consult your diagram to figure out what swarch-type DEs the new RE can see. Determine routes out of the RE a call can be processed, and identify DEs for all routes.

2 If any of those DEs are not in swarch, add them to swarch by using "Add to Swarch (or other "arch") Table" (p. 4-61) .

3 Use the procedure "Map an RE to its swarch DEs" (p. 4-68) , to Map the RE to each swarch-type DE. Do this in the RE's routing table. For example, if the RE is a 5ESS from a 5ESS conversion, **dbedit** route5e.

Important! With some conversions, routing tables are not used. See "Map an RE to its swarch DEs" (p. 4-68) .

4 Continue with the next procedure.

END OF STEPS

Procedure: Add the new RE as DEs

1 Consult your diagram to figure out what existing REs see the new RE as a DE.

2 Complete "Procedure: Add the RE's swarch-type DEs, and map the RE to those DEs" (p. 4-19) , but in the opposite direction. That is, add the new RE to the routing table of each existing RE that sees it as a DE.

Example: If an existing 1AESS RE sees the new 5ESS RE as a DE, **dbedit** route1a.

3 Continue with the next procedure.

END OF STEPS

Procedure: Add the SCPs and map SCPs and STPs

1 Normally, you should have added STPs and SCPs first before other REs. However, at this point you can check.

Go to "Tables to dbedit to add an RE" (p. 4-25) . Look in the column for the RE's conversion, at the scparch row. Is there a "2"?

- If no, go to the next step.
- If yes use the procedure in "Add and Map SCPs and STPs" (p. 4-32) . If you are mapping to an existing SCP, refer to "Add and Map SCPs and STPs" (p. 4-32) (and you may need to do nothing).

2 Continue with the next procedure.

END OF STEPS

Procedure: Conversion Specifics

1 Go to "Add an RE, conversion specifics" (p. 4-22) . Then return here.

2 Continue with the next procedure.

END OF STEPS

Procedure: Test and Monitor

1 To ensure CIMs are arriving from the switch, and are being changed to CFIMs, enter (here switch 2222222222 is being checked):

```
sui find source=cfim search=re=2222222222
```

or

```
sui trapcfim re=2222222
```

Important! Look for CFIMs with the current date. If you see no data after 5 to 10 minutes, check the log files in $LOGDATA to see if data is being discarded. See also "Monitor Links" (p. 5-51) for more on monitoring data links.

2 Use the operating system **cat** command or a text editor (such as **vi**) to view the latest incon (inconsistency) log.

Example

- Go to the **$LOGDATA** directory and list the contents to find incon logs
- Use a text editor (such as **vi**) to view the incon log with the most recent timestamp (in incon234.02.30, for example, the 234.02.30 is the julian date and time of the first message in the file).
- A message resembling the following tells you that the record for switch clmbohxxcg0 in the swarch table needs a value in its hnpa field. Use **dbedit** to correct the record in the swarch table.

```
Tue Jun 24 12:58:41 2003 HP-UX:9000/891:io_cp1:ntp

Incon.C:121

ERR002 EVENT No HNPA for "clmbohxxcg0" in swarch
```

Reference: See "incon Log" (p. 10-29) .

3 For a new 4ESS RE (only), make a note to watch for CFIM's where the new 4ESS is RE, and the Rt field is incorrect. This can happen if the 4ESS talks to new DEs not in the de2route table.

Reference: "Correct Wrong or Missing Rt Values" (p. 4-52) .

END OF STEPS

Add an RE, conversion specifics

This is a sub-task of "Add an RE" (p. 4-17) . When you finish here, return to "Procedure: Conversion Specifics" (p. 4-21) . This sub-task requires you to know the RE's conversion (see "Figure out what conversion to use" (p. 4-16)).

If Conversion is	Do this
1AESS	NA
4ESS	• If you implemented Adjuncts, and the new RE sees them as DEs, see "Add an adjunct as DE" (p. 4-44) . If the RE sees existing adjuncts as REs, see "Procedure: Add the RE's swarch-type DEs, and map the RE to those DEs" (p. 4-19) (in this case, you may need to do nothing). • If you implemented ECOS areas, and the new RE sees them as DE's see "Add an ECOS area as DE" (p. 4-47) . If the RE sees existing ECOS areas as RE's see "Add an adjunct as DE" (p. 4-44) (in this case, you may need to do nothing).
5ESS	IF the switch is a 5ESS, and IF it is in generic 5E12 or later, ask the switch administrator if the switch has multiple PCs (point codes). In other words, does it have, not only a PC address for the switch, but also, one or more additional PC address for remote switching modules? If it does, use **`dbedit`** to, put the switch CLLI, and each of its PCs in the pc2clli table. See "pc2clli Table" (p. A-123) for an illustration.
7R/E PLS	NA

If Conversion is	Do this
AUTOPLEX MSC	This is a wireless switch with four components, ECP, 5ESS modules, cell base stations, and location registers. Add both ECPs and 5ESS modules as RE as follows: • ECP RE. Add the following as DEs: – Its own 5ESS modules. Use "Procedure: Add the RE's swarch-type DEs, and map the RE to those DEs" (p. 4-19) . – Locations registers. Use "Add a location register as a DE" (p. 4-38) . – Cell base stations. Use "Add a cell base station" (p. 4-42) . • Its own 5ESS modules REs, with PSTN switches as DEs. Use "Add an RE" (p. 4-17) . (In other words, use this procedure again for each 5ESS module.)
DMS MTX MSC and DMS MSC (GSM)	This is a wireless switch. It sees as DEs its cell base stations. To add them as DEs, see "Add a cell base station" (p. 4-42) .
OTR (DMS TOPS module)	See "OTR FDCs" (p. 4-90) . **dbedit** the lrn2ne and lrarch tables, so NTP can fill in the CFIM's Lrn field. See "lrn2ne Table" (p. A-92) and "num_std_rule Table" (p. A-116) .
OTR (5ESS OSPS module)	See "OTR FDCs" (p. 4-90) .
DMS	NA
EWSD	NA
Sucesion SN05 and SN06	NA
GeoProbe	This RE is in swarch and rearch. DEs are NOT in swarch, any other "arch", or any routing table. Also, scparch and scproute are not used, though univlog is used. However, you do need to identify the new RE's DE's by getting their CLLIs and point codes (from the GeoProbe administrator, or maybe from messages in the incon or univlog log), and using **dbedit** to add them to the pc2clli table. (In that table, add the new RE's clli and point code too, so other REs can see it as a DE. Please note the following: • Point codes arrive in GeoProbe CIMs' OPC and DPC fields. You populate pc2clli so NTP knows how to convert them to CLLIs. • You do NOT need to add the new RE and its DEs to route tables (such as dmsroute), or "arch" tables (such as scparch) other than swarch. GeoProbe conversion does not use those tables.

If Conversion is	Do this
AXE 10	Add RE (and its DEs) to the id2ne table. DE's are NOT in swarch, any other "arch", or any routing table, but are taken from CDRs. Also, scparch and scproute are not used.
AXE 10 TRADO	NA
Lucent Softswitch	**`dbedit`** the lrn2ne and lrarch tables, so NTP can fill in the CFIM's Lrn field. See "lrn2ne Table" (p. A-92) and "num_std_rule Table" (p. A-116) .
IPDRs	DEs in swarch need ipaddress field filled in. No routing table used for DEs.
Any from a consultant-added CDR conversion	NA

Tables to Edit to Add an RE

Tables to dbedit to add an RE

This table lists all NTP databases you must dbedit when adding an RE. Tables shown for enhanced CDR analysis may be used in consultant-configured configurable converter installations.

Legend

- *1 — dbedit* the table before adding the FIRST RE (when setting up the interface), and edit again only if needed. Many of these tables are pre-filled, and you need only verify they are current.
- *2 — dbedit* the table for EACH RE.
- *Grey blocks* — information to be determined.

Reference: For tables used to add CIM sources, see "Description" (p. 5-12). Some sources can collect and forward data from multiple REs. For some direct interfaces, however, you must add a unique source for EACH RE.

Table	1AESS	4ESS	5ESS and 7R/E PLS	AUTOPLEX MSC and GPRS	DMS MTX MSC	OTR (5ESS OSPS, DMS TOPS)	DMS	DMS MSC	EWSD	EVDO PCMD	Alcatel S1240	Succession SN05 and SN06	GeoProbe	AXE 10 and Ericsson GSM	AXE 10 TRADO	Lucent Softswitch	IPDRs	Consultant-Added CDR	CCF Charging Collection Function	Sonus	SIP Log	SDHLR OM	Alcatel 5020 Softswitch	BroadWorks® Broadsoft® FS3000	IMS Charging Record Support	Motorola iDEN Support
acode2fdc	-	-	-	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	-	1
adjarch	-	2	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
adjroute	-	2	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
carrier	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-
cellroute	-	-	-	2	2	-	-	2	-	-	-	-	-	2	-	-	-	-	-	-	-	-	2	-	-	-
celltype	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
city	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	1	1	1	1	-	1	-	-	-
code2text	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
cos	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Table	1AESS	4ESS	5ESS and 7R/E PLS	AUTOPLEX MSC and GPRS	DMS MTX MSC	OTR (5ESS OSPS, DMS TOPS)	DMS	DMS MSC	EWSD	EVDO PCMD	Alcatel S1240	Succession SN05 and SN06	GeoProbe	AXE 10 and Ericsson GSM	AXE 10 TRADO	Lucent Softswitch	IPDRs	Consultant-Added CDR	CCF Charging Collection Function	Sonus	SIP Log	SDHLR OM	Alcatel 5020 Softswitch	BroadWorks® Broadsoft® FS3000	IMS Charging Record Support	Motorola iDEN Support
country	-	1	-	-	-	-	-	-	-	-	-	-	1	-	-	1	-	1	1	1	1	-	1	-	-	-
count_def	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1
ctcode2ct	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	1	1	-	1	-	-	-	-	-	-
custcode	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	1	-	-	-	-	-	-	-	-
custid	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	1	-	-
custip	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-
customer	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-
dcode2d	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-
de2route	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
disabledig	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-
dmsroute	-	-	-	-	2	-	2	2	-	-	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-
domain	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
ecosarch	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
ecosroute	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
eqtype	1	1	1	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	-	-	-	-	1	1	-	1
ess1a2fdc	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
ewsdroute	-	-	-	-	-	-	-	-	2	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
fdc	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	-	1
fdc2tn	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
fdcgroup (optional)	1	1	1	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	-	-	-	-	1	-	-	-
fdcgroupmap (optional)	1	1	1	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	-	1	-	-	-	-	-	-

Table	1AESS	4ESS	5ESS and 7R/E PLS	AUTOPLEX MSC and GPRS	DMS MTX MSC	OTR (5ESS OSPS, DMS TOPS)	DMS	DMS MSC	EWSD	EVDO PCMD	Alcatel S1240	Succession SN05 and SN06	GeoProbe	AXE 10 and Ericsson GSM	AXE 10 TRADO	Lucent Softswitch	IPDRs	Consultant-Added CDR	CCF Charging Collection Function	Sonus	SIP Log	SDHLR OM	Alcatel 5020 Softswitch	BroadWorks® Broadsoft® FS3000	IMS Charging Record Support	Motorola iDEN Support
fdcpermit (optional)	1	1	1	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	-	1	-	-	-	-	-	-
gtspec (GTT translations only)	1	1	1	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	-	-	-	-	-	-	-	-
homedigits (custom configurations)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-
id2ne	-	-	-	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-	-	-	-	-	-	-	-
iparch (May be used for IPDR, which normally uses swarch.)	-	-	2	2	(GPRS)		-	-	-	-	-	-	-	-	-	-	2	2	1	-	1	-	-	1	2	-
ixcarrier	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	1	-	-	-	-	-	-	-	-
latacode	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-
lrarch	-	-	-	2	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
lrn2ne	-	-	-	2	2	-	-	-	-	-	-	-	-	-	-	2	-	-	-	2	-	-	2	-	-	-
netsegmap (For new RE's; might modify other "net" tables not listed here.)	2	2	2	2	2	2	2	2	2	-	2	2	2	2	2	2	2	2	-	-	-	-	-	-	-	-
npt	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
oline2st	-	-	-	-	-	-	-	-	1	-	1	-	1	-	-	-	1	1	-	1	-	-	-	-	-	-
otr2fdc	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
owner	1	1	1	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	-	1	-	-	-	-	1	-

Table	1AESS	4ESS	5ESS and 7R/E PLS	AUTOPLEX MSC and GPRS	DMS MTX MSC	OTR (5ESS OSPS, DMS TOPS)	DMS	DMS MSC	EWSD	EVDO PCMD	Alcatel S1240	Succession SN05 and SN06	GeoProbe	AXE 10 and Ericsson GSM	AXE 10 TRADO	Lucent Softswitch	IPDRs	Consultant-Added CDR	CCF Charging Collection Function	Sonus	SIP Log	SDHLR OM	Alcatel 5020 Softswitch	BroadWorks® Broadsoft® FS3000	IMS Charging Record Support	Motorola iDEN Support
pc2clli (5ESS switches only if they have multiple point codes.)	-	-	2	2	-	-	-	-	-	-	-	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-
potsroute	-	-	-	2	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
psxid2name	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-	-
rearch	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	2	1	1	2	1	2	2
route1a	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
route5e	-	-	2	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
rtarch	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
s1240route	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
samplingrate	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
scparch	-	2	-	-	2	-	2	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
scproute (may be needed for RE's using a BILLDATS source)	-	2	-	-	2	-	2	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
scode2sig	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-
sdthresh (For optional system day thresholding; always applies to OTR.)	2	2	2	2	2	2	2	2	2	-	2	2	2	2	-	-	-	-	-	-	-	-	-	-	-	-
sdttype	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
sensor2clii	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	2	-	-

Table	1AESS	4ESS	5ESS and 7R/E PLS	AUTOPLEX MSC and GPRS	DMS MTX MSC	OTR (5ESS OSPS, DMS TOPS)	DMS	DMS MSC	EWSD	EVDO PCMD	Alcatel S1240	Succession SN05 and SN06	GeoProbe	AXE 10 and Ericsson GSM	AXE 10 TRADO	Lucent Softswitch	IPDRs	Consultant-Added CDR	CCF Charging Collection Function	Sonus	SIP Log	SDHLR OM	Alcatel 5020 Softswitch	BroadWorks® Broadsoft® FS3000	IMS Charging Record Support	Motorola iDEN Support
signaling	1	1	1	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	-	-	-	-	-	-	-	-
signet		1	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
st	-	-		1	-	-	-	-	1	-	1	-	1	1	1	1	1	1	-	-	-	-	-	-	-	-
stcode2st	-	-	-	1 (GPRS)	-	-	-	-	-	-	-	-	-	1	1	1	1	1	-	1	-	-	1	-	-	-
stparch (may be used in some CDR installations)	1	1	1	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	-	-	-	-	-	-	-	-
swarch	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	2	1	1	2	2	2	2
tcapdiag	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
univroute	-	-	-	-	-	-	-	2	-	-	-	2	-	2	2	2	-	2	-	-	-	-	2	-	-	-
vpnid (for custom configurations)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-
vpnroute (for custom configurations)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-

Defining REs associated with IMS components

Purpose

Administrators need to provide entries into IMS-related reference tables documented in Appendix A.

It is advisable to establish a naming convention when adding REs associated with any IMS component.

Each RE should have a unique name, which is useful for readability of all rendered performance data. The naming scheme is not essential; it just needs to be meaningful to you.

Add DE-Only Elements

Overview

Purpose

Definition

Use procedures in this section so DE-only elements can show up in CFIMs' DE fields.

- SCPs (signal control points) — mapped to RE's and STPs
- AUTOPLEX —
  - Location register
  - Cell base station (also for DMS-MTX)
- Adjuncts
- ECOS area

Contents

Add and Map SCPs and STPs

Purpose

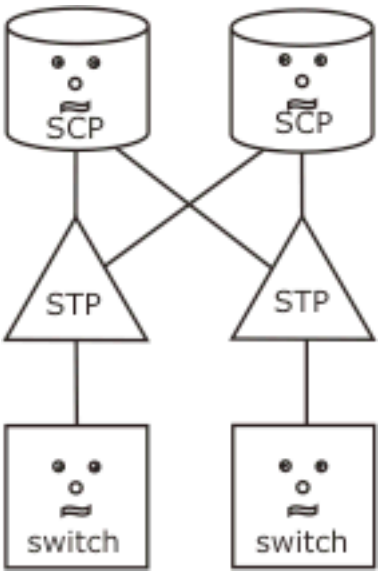
This procedure tells how to add SCPs, and how to map SCPs to REs and STPs, so that:

- SCPs can appear as DEs on CFIMs. (An SCP can not be an RE, since it does not create CIMs.)
- STPs can appear in the CFIM Rs and Ds fields.

The main table we *dbedit* in this procedure is scproute.

SCP and STP illustration

An SCP is actually a pair of databases, used by a pair of STPs (signal transfer points), which supply signalling (SS7) to network elements such as switches.



STPs

Although you might think of STPs (signal transfer points) as another non-switch network element, NTP treats them differently, as follows:

- There is no STP type in the eqtype table. Instead, each STP is listed in the stparch table.
- On CFIMs, STPs do not appear in DE, or Related fields. Instead they are in Rs (reporting STP) and Ds (distant STP) fields.
- Adding STPs happens when you add SCPs (or other non-switches).
- STPs are not thresholded.

Which conversions use this

Go to “Tables to dbedit to add an RE” (p. 4-25). Look in the column for your RE's conversion, at the scparch row. Is there a "2" there? If yes, use this procedure when needed to add SCPs, and to map SCPs to STPs and RE's.

Add an SCP as DE

Purpose

This procedure tells how to add SCPs, and how to map SCPs to REs and STPs.

Reference: To edit files in this procedure you can use any ASCII text editor, such as *vi* . For more information on using *vi* , see "Edit (vi) ASCII Files" (p. 3-13) .

Procedure

Use this procedure to add a new SCP as a DE for existing RE's.

1 To make a template record for the scparch table, enter

```
sui find source=scparch noheader delim='";"' maxsave=1 > temp
```

2 Use a text editor (such as *vi*) to open the temp file.

The file resembles this:

```
#Scpclli
;Mateclli;Dpc;Stp;Ai

sv0apasla15;sv0bpadga15;122-101-122;sv0b;on
```

3 Change the second line to represent the SCP you are adding, and save the file.

Reference: For what to put in each field of the scparch table, see "scparch Table" (p. A-137) .

4 To insert the record from the temp file into the scparch table, enter

```
dbedit -i -t scparch -f temp -s";"
```

5 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see "Correct dbedit Errors" (p. 3-27) .

6 To verify the CLLI is in scparch, enter (this example is for CLLI 22222222222):

```
sui find source=scparch search=scpclli=22222222222
```

7 Remove the temp file.

8 Is there more than one SCP in the network?

- If NO go to Step 16.
- If YES, you need to use the scproute table to map which 800 and 888 numbers go to each SCP. Go to the next step.

9 To make a template record for the scproute table, enter

```
sui find source=scproute noheader delim='";"' maxsave=1 > temp
```

10 Use a text editor (such as *vi*) to open the temp file, change the line to what you are adding, and save the file.

The file resembles this:

```
122122;sv1admscp01
```

Reference: For what to put in each field of the scproute table, see "scproute Table" (p. A-138) .

11 To insert the record from the temp file into the scproute table, enter

```
dbedit -i -t scproute -f temp -s";"
```

12 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see "Correct dbedit Errors" (p. 3-27) .

13 To verify the CLLI is in scproute, enter (this example is for scpclli 22222222222):

```
sui find source=scproute search=scpclli=22222222222
```

14 Remove the temp file.

15 You may also need to add entries into the gtspec table to find DEs.

Important! Review Chapter 11, "Update the gtspec Table" before attempting to make changes to the gtspec table.

16 To add the SCP to any network groups or segments you want it to belong to, see "Modify a network group or segment" (p. 7-40) .

END OF STEPS

Add an AUTOPLEX Location Register as DE

Purpose

A location register is a database used for authenticating AUTOPLEX (wireless) calls. This section tells how to add an AUTOPLEX location register. These can show up on CFIMs as DEs only, and only on CFIMs from AUTOPLEX switches.

REs and DEs

With the Autoplex conversion, you may see four types of elements.

Element	Purpose	On CFIMs from AUTOPLEX switches, seen in this field:	Reference
ECP (executive cellular processor)	Governs the AUTOPLEX	RE (it sees as DE's its own 5ESS modules, location registers, or cell base station)	"Add an RE" (p. 4-17)
5ESS switch modules within AUTOPLEX	Connect the AUTOPLEX to the PSTN	• RE (it sees as DE's switches in the PSTN) • DE (as seen by the ECP)	"Add an RE" (p. 4-17),
Location registers	Databases for authenticating wireless calls.	DE (as seen by the ECP)	"Add an AUTOPLEX Location Register as DE" (p. 4-37)
Cell base stations	Grouping of radios and other hardware for wireless calls.	DE (as seen by the ECP)	"Add an Cell Base Station as DE" (p. 4-40)

First-time

The following are one-time changes that must be made before the first AUTOPLEX location register can be added.

What to do	Note	Reference
Create the lrarch table	This is done automatically, when you load NTP software. You populate this table in "Add a location register as a DE" (p. 4-38).	"lrarch Table" (p. A-91)

Add a location register as a DE

Purpose

This section tells how to add an AUTOPLEX location register. These can show up on CFIMs as DEs only, and only on CFIMs from AUTOPLEX switches

Reference: To edit files in this procedure you can use any ASCII text editor, such as *vi* . For more information on using *vi* , see “Edit (vi) ASCII Files” (p. 3-13) .

Procedure

Use this procedure to add a new location register as a DE for AUTOPLEX REs.

1 Add to the lrarch table by doing the following:

To make a template record for the lrarch table, enter

```
sui find source=lrarch noheader delim='";"' maxsave=1 > temp
```

2 Use a text editor (such as *vi*) to open the temp file.

The file resembles this:

```
#Clli;Dpc;Ai

svohlr01;122-101-122;on
```

3 Change the second line to represent the location register you are adding, and save the file.

Reference: For what to put in each field of the lrarch table, see “num_std_rule Table” (p. A-116) .

4 To insert the record from the temp file into the lrarch table, enter

```
dbedit -i -t lrarch -f temp -s";"
```

If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see “Correct dbedit Errors” (p. 3-27) .

5 To verify the CLLI is in lrarch, enter (this example uses CLLI 22222222222):

```
sui find source=lrarch search=clli=22222222222
```

6 Remove the temp file.

7 UN-Map location registers DEs to MSC REs.

There is no "location register route" table. Instead, use:

- route5e table to un-map location register REs from AUTOPLEX MSC REs
- dmsroute table to un-map location register REs from DMS-MTX MSC REs

8 Add to the netsegmap and netgroupmap tables

9 To add the location register to any network groups or segments you want it to belong to, see “Modify a network group or segment” (p. 7-40) .

Important! If you create a network group of location registers, their type is lr.

END OF STEPS

Add an Cell Base Station as DE

Purpose

A cell base station is a collection of radios and other hardware for wireless switching, usually located next to an antenna. This section tells how to add a cell base station so it can show up on CFIMs as DEs.

You see cell base stations as DEs only on CFIMs where the RE is a wireless switch—either:

- AUTOPLEX
- DMS MTX
- DMS MSC

REs and DEs

For what AUTOPLEX MSC conversion sees as REs and DEs, see "REs and DEs" (p. 4-37).

DMS MTX MSC conversion sees the following as REs and DEs.

Element	Purpose	On CFIMs from DMS MTX switches, seen in this field:	Reference
DMS MTX switch (as a whole, not by DMS modules) and DMS MSC	Wireless switch	RE	"Add an RE" (p. 4-17)
Cell base stations	Grouping of radios and other hardware for wireless calls.	DE	"Add an Cell Base Station as DE" (p. 4-40)

First time

The following is a one-time change that must be made before the first cell base station can be added.

What to do	Note	Reference
Create the cellroute table.	This is done automatically, when you load NTP software. You populate this table in "Add a cell base station" (p. 4-42).	"cellroute Table" (p. A-34)

What to do	Note	Reference
Add "base" to the eqtype table. Do this so you can put base in the eqtype field of the swarch table for each cell base station in that table. Something similar is NOT done for location registers, since they are identified by being in the lrarch table. (Cell base stations are the only non-switches in swarch. There is no cellarch table.)	The general procedure for updating a table is in "dbedit Insert or Update Example" (p. 3-32).	"eqtype Table" (p. A-62)

Add a cell base station

Purpose

This section tells how to add a cell base station so it can show up on CFIMs as DEs.

Reference: To edit files in this procedure you can use any ASCII text editor, such as *vi* . For more information on using vi, see “Edit (vi) ASCII Files” (p. 3-13) .

Procedure

Use this procedure to add a new cell base station as a DE for AUTOPLEX or DMS MTX/DMS MSC REs.

1 Add to the swarch table

Use the procedure in “Add to Swarch (or other "arch") Table” (p. 4-61) to see if the new CLLI is in swarch, and add it if it is not.

> **Important!** Put base in the eqtype field of the swarch table. If you fail to do this, the system will run normally, but you may have trouble identifying which CLLIs in swarch belong to cell base stations.

2 Add to the cellroute table

To make a template record for the cellroute table, enter

```
sui find source=cellroute noheader delim='";"' maxsave=1 > temp
```

3 Use a text editor (such as vi) to open the temp file.

For a DMS MTX, the file entry resembles this:

```
#Clli;Cell;Detype;DE

sv0cbauto01;121;cell;sv0gdi5e001
```

For a DMS MSC, the file entry resembles this:

```
#Clli;Cell;Detype;DE

gcpknyaicm0;1000-1;cell;gcp1-1000-1

gcpknyaicm0;35026-471;cell;gcp1-35026-471
```

For the DMS MSC:

- the Cell field entry consists of <lac> - <cell number> <lac> is the location area code.
- the DE entry consists of the <nealias>-<lac>-<cell number>
  where <nealias> is 4 character abbreviation for a switch defined in the searchalias table.

  Important! The DE referred to in the cellroute table should be defined in swarch.

4 Change the second line to what you are adding, and save the file.

  Important! For what to put in each field of the cellroute table, see "cellroute Table" (p. A-34) .

5 To insert the record from the temp file into the cellroute table, enter
`dbedit -i -t cellroute -f temp -s";"`

6 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see "Correct dbedit Errors" (p. 3-27) .

7 To verify the CLLI is in cellroute, enter (this example uses CLLI 22222222222):
`sui find source=cellroute search=clli=22222222222`

8 Remove the temp file.

9 Add to the netsegmap and netgroupmap table

To add the cell base station to any network groups or segments you want it to belong to, see "Modify a network group or segment" (p. 7-40) .

Important! If you create a network group of cell base stations, their type is cell.

END OF STEPS

Add an adjunct as DE

Purpose

Adjunct switches are modules that reside on another switch but are treated as separate network entities. Use this procedure to add a new adjunct as a DE. You can NOT add an adjunct as an RE.

Procedure

Use this procedure to add an adjunct as a DE. *Reference:* To edit files in this procedure you can use any ASCII text editor, such as *vi* . For more information on using *vi* , see “Edit (vi) ASCII Files” (p. 3-13) .

1 Add to the adjarch table

To make a template record for the adjarch table, enter

```
sui find source=adjarch noheader delim='";"' maxsave=1 > temp
```

2 Use a text editor (such as vi) to open the temp file.

The file resembles this:

```
#Adjclli;Dpc;Type;Swclli;Stp;Ai
sv0prfadj59;-;nscx;sv0prfdm184;sv0p;on
```

3 Change the second line to the adjunct you are adding, and save the file.

Reference: For what to put in each field of the adjarch table, see “adjarch Table” (p. A-13) .

4 To insert the record from the temp file into the adjarch table, enter

```
dbedit -i -t adjarch -f temp -s";"
```

5 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see “Correct dbedit Errors” (p. 3-27) .

6 To verify the CLLI is in adjarch, enter (this example uses CLLI 22222222222):

```
sui find source=adjunct search=adjclli=22222222222
```

7 Remove the temp file.

8 Add to the adjroute table

Add the same CLLI to the adjroute table. To make a template record for the adjroute table, enter

```
sui find source=adjroute noheader delim='";"' maxsave=1 > temp
```

9 Use a text editor (such as vi) to open the temp file.

The file resembles this:

```
#Digits;Adjclli
179;sv0prfadj28
```

10 Change the second line to the adjunct you are adding, and save the file.

Reference: For what to put in each field of the adjroute table, see "adjroute Table" (p. A-14) .

11 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see "Correct dbedit Errors" (p. 3-27) .

12 To verify the CLLI is in adjroute, enter (this example uses CLLI 22222222222):

```
sui find source=adjroute search=adjclli=22222222222
```

13 Remove the temp file.

14 Add to the netsegmap and netgroupmap tables

To add the adjunct to any network groups or segments you want it to belong to, see "Modify a network group or segment" (p. 7-40) .

15 Add to the gtspec table

If the addition of the adjclli affected the gtspec table, update that table.

Important! Review Chapter 11, "Update the gtspec Table" before attempting to make changes to the gtspec table.

END OF STEPS

Add an ECOS area as DE

Purpose

ECOS (End-to-End Class of Service) is a way to group calls by some criteria, so NTP can treat each grouping (called an "area") as if it were a DE. Use this procedure to add a new ECOS area as a DE for existing RE's. You can not add an ECOS area as an RE.

Reference: To edit files in this procedure you can use any ASCII text editor, such as *vi* . For more information on using *vi* , see "Edit (vi) ASCII Files" (p. 3-13) .

Procedure

Use this procedure to add an ECOS area as a DE.

1 Add to the ecosarch table

To make a template record for the ecosarch table, enter

```
sui find source=ecosarch noheader delim='";"' maxsave=1 > temp
```

2 Use a text editor (such as *vi*) to open the temp file.

The file resembles this:

```
#Area;Ai

sv0ecos0001;on
```

3 Change the second line to the ECOS area you are adding, and save the file.

Important! For what to put in each field of the ecosarch table, see "ecosroute Table" (p. A-61) .

4 To insert the record from the temp file into ecosarch, enter

```
dbedit -i -t ecosarch -f temp -s";"
```

5 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see "Correct dbedit Errors" (p. 3-27) .

6 To verify the CLLI is in ecosarch, enter (this example uses CLLI 22222222222):

```
sui find source=ecosarch search=area=22222222222
```

7 Remove the temp file.

8 Add to the ecosroute table

To make a template record for the ecosroute table, enter

```
sui find source=ecosroute noheader delim='";"' maxsave=1 > temp
```

9 Use a text editor (such as *vi*) to open the temp file.

The file resembles this:

```
#Ro;Areaid;Area

sv0alt00001;234;sv0ecos000
```

10 Change the second line to the ECOS area you are adding, and save the file,

Reference: For what to put in each field of the ecosroute table, see "ecosroute Table" (p. A-61) .

11 To insert the record from the temp file into ecosroute, enter

```
dbedit -i -t ecosroute -f temp -s";"
```

12 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see "Correct dbedit Errors" (p. 3-27) .

13 To verify the CLLI is in ecosroute, enter (this example uses adjclli 22222222222):

```
sui find source=ecosroute search=adjclli=22222222222
```

14 Remove the temp file.

END OF STEPS

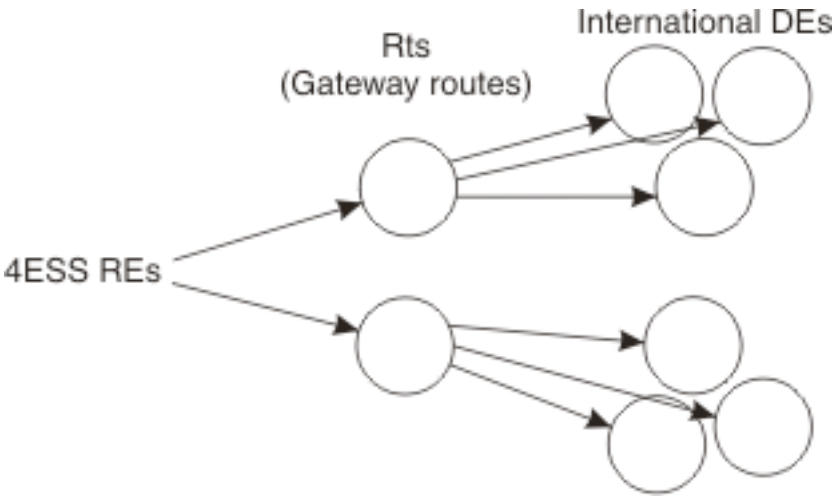
Rts

Overview

Purpose

Rt illustration

RE, Rt, and DE are CFIM fields. An Rt is a gateway route, which is a switch between an RE and an international DE, illustrated here.



This section tells how to correct problems that cause Rt values to be wrong or missing on CFIMs.

Note

- You will see values in a CFIM's Rt field only if the CFIM's Retype field says 4ESS.
- Alerting lets you threshold on the Rt field. See Chapter 8, “Threshold Administration” .

Table overview

For Rt's to appear on CFIMs, two tables must be populated. Both are populated during installation by your NTP support organization.

Table	Purpose	How often to update
Rtarch	Names Rt's.	Rarely. Only if an Rt is added or removed.

Table	Purpose	How often to update
De2route	Maps each international DE to an Rt.	Often. Each time Rt-DE routing changes.

Contents

Correct Wrong or Missing Rt Values

Purpose

This section tells what to do if you see wrong or missing values in a CFIM's Rt field.

When to use

Use this procedure when a CFIM's Rt value is:

- **`Wrong`**. Rt values can often be wrong, since Rt-to-DE assignments may change. See network managers for current Rt-to-DE routing, and check the De2route table. To see De2route records, enter

  ```
  sui find source=de2route
  ```

- **`Missing`**. Rt values can be missing. A missing Rt value is NOT indicated by a "?" in Rt, but by "-" in Rt when Ccd is NOT "-". So, to list CFIMs with missing Rt values, enter

  ```
  sui find source=cfim search=ccd!="-" AND search=rt="-"
  ```

  Then use this procedure for each unique DE on output.

  Important! NEMOS can be a source to get Rt-DE assignments from NEMOS. See your NTP support organization for details.

Correct wrong or missing Rt values

Purpose

This procedure tells you how to correct wrong or missing values in a CFIM's Rt field.

Procedure

Use this procedure to correct wrong or missing Rt values on CFIMs. *Reference:* To edit files in this procedure you can use any ASCII text editor, such as *vi* . For more information on using *vi* , see “Edit (vi) ASCII Files” (p. 3-13) .

1 Get correct Rt-DE pair information (see “When to use” (p. 4-56)).

2 Verify that the Rt (of the Rt-DE pare you are correcting) is already in the Rtarch table.

Example: To list all Rt's in Rtarch, enter:

```
sui find source=rtarch
```

3 Is the Rt in Rtarch? If:

- YES, go to the next step.
- NO, go to “Add an Rt” (p. 4-56)

Important! Since Rt is populated only on CIMs where REs are 4ESS, DEs do not need to be in Swarch (4ESS DEs are in the CIMs).

4 If you need to:

- Add a new Rt-DE pair, go to the next step.
- Modify an existing Rt-DE pair, go to the next step.
- Delete an Rt-DE pair, go to Step 10.

5 Add or modify an Rt-DE pair

To:

- *Add* . Make a template record for the De2route table. Enter
  ```
  sui find source=de2route noheader delim='";"' maxsave=1 > temp
  ```
- *Modify* . Using the DE as your key, retrieve the record you want to modify.

Example: To modify the record where RE is rtparis (and Rt is anything), enter

```
sui find source=de2route search=de=hamburg12345 noheader
delim='";"' > temp
```

6 Use a text editor (such as vi) to open the temp file.

The file resembles this:

```
#DE;Rt

hamburg12345;rtparis
```

7 Change the record to the DE and Rt you want, and save the file

Important! A given DE can appear in only one record.

Reference: For what to put in each field of the Rtarch table, see "de2route Table" (p. A-55)

8 To update or insert the record from the temp file into de2route, enter

```
dbedit -ui -t de2route -f temp -s";"
```

9 Go to Step 13.

10 To delete an Rt-DE pair, using the DE as your key, make a delete file.

Example: To delete the record where DE is hamburg12345 (and Rt is anything), enter

```
sui find source=de2route search=de=hamburg12345 noheader
delim='";"' > temp
```

11 Use the operating system **cat** command or a text editor (such as vi) to verify temp holds the correct DE.

The temp file resembles this:

```
#DE;Rt

hamburg12345;rtparis
```

12 To delete the record, enter **dbedit -d -t rtarch -f temp -s";"**

13 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see “Correct dbedit Errors” (p. 3-27) .

14 To verify the record was added, corrected, or deleted, enter (this example uses DE of hamburg12345):

sui find source=de2route search=de=hamburg12345

15 Remove the temp file.

END OF STEPS

Add an Rt

Purpose

This section tells how to add an Rt to the rtarch table.

When to use

Use this if you discover a new Rt (for example, in Step 3 of "Correct wrong or missing Rt values" (p. 4-53)).

Procedure

Use this procedure to add an new Rt. *Reference:* To edit files in this procedure you can use any ASCII text editor, such as *vi* . For more information on using *vi* , see "Edit (vi) ASCII Files" (p. 3-13) .

1 Make a template record for the rtarch table, enter

```
sui find source=rtarch noheader delim='";"' maxsave=1 > temp
```

2 Use a text editor (such as *vi*) to open the temp file.

The file resembles this:

```
#Rt

london1rt
```

3 Change the second line to the Rt you are adding, and save the file.

Important! The rt field must contain a unique value which is not defined in a field in one of the following tables:

- swarch.clli
- stparch.ne
- lrarch.clli
- adjarch.adjclli
- ecosarch.area

Reference: For what to put in each field of the Rtarch table, see "rtarch Table" (p. A-134) .

4 To insert the record from the temp file into Rtarch, enter

```
dbedit -i -t rtarch -f temp -s";"
```

5 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see "Correct dbedit Errors" (p. 3-27) .

6 Verify the record is added.

Example: To verify rtparis is add in rtarch, enter

```
sui find source=rtarch search=rt=rtparis
```

7 Remove the temp file.

END OF STEPS

Trunk Group Suffix (Sfx)

Purpose

The Trunk Group Suffix feature provides the infrastructure to populate a suffix field (*sfx*) for all *cfim* converters that populate an external trunk group identifier. It improves the ease of use of NTP in environments where 8920 Network Traffic Management (NTM) software is also used.

The following converters have been updated:

- 5ESS (MDII)
- DMS
- *Sonus*
- EWSD
- GTD5.

NTM perspective

NTM identifies trunk groups with 3 pieces of information:

- from-office (near-end),
- to-office (far-end), and
- suffix (a user-defined string, up to 8 characters long, used to identify a particular trunk group).
  *Example:*NTM could have the following 911 trunk group defined:

```
FROM: clmboh12ds0

TO: clmboh14ds0

SFX: e911
```

NTP perspective

NTP normally identifies trunk groups with 2 pieces of information: RE (Reporting Entity - near-end) and DE (Distant Entity - far-end). This optional feature adds a suffix for NTP trunk group identification.

Example: With this feature the trunk group could be represented as follows:

```
RE: clmboh12ds0

DE: clmboh14ds0

SFX: e911
```

Shared Procedures

Purpose

Purpose

This section gives procedures called from other procedures in this chapter.

Backup

Before modifying any table, it is recommended that you make a backup ASCII copy of the table.

Example: To make a backup ASCII copy of swarch, enter

```
sui find source=swarch noheader delim='";"' max=100000> hold_swarch
```

Ai fields

If you *dbedit* a record that has an ai (alert indicator) field, it is recommended that you initially set it to off. Then, after verifying NTP is collecting data and processing it to CFIMs for all intervals, *dbedit* again to make it on, to start thresholding.

Add to Swarch (or other "arch") Table

When to use

Use this procedure to add elements to all "arch" tables except rearch. That is, to add to swarch, lrarch, and other "arch" tables listed in the second column of the table at “"Arch" and route tables” (p. 4-7).

Important! If your network has SCPs or STPs, you must add them first. Otherwise you can't add the appropriate information for these elements in the swarch table.

Before you begin

Before an entity can be added to the swarch (or other "arch") table, its equipment type must be in the eqtype table. To see this table, enter

`sui find source=eqtype.`

Add to swarch or other "arch" table

Purpose

Use this procedure to add an entity to the swarch table. If using this procedure to add a non-switch entity to another "arch" type table, substitute that table name in place of swarch in this procedure.

Reference: To edit files in this procedure you can use any ASCII text editor, such as *vi* . For more information on using *vi* , see “Edit (vi) ASCII Files” (p. 3-13) .

Procedure

Use this procedure to add an entity to the swarch table.

1 See if the entity is already in the swarch table.

Example: If the entity's CLLI is 22222222222, enter

```
sui find source=swarch search=clli=22222222222
```

2 Is the CLLI in the swarch table?

- If YES, STOP. You are done
- If NO, go to the next step.

3 Enter **`sui find source=swarch noheader delim='";"' maxsave=1 > temp`**

4 Use a text editor (such as vi) to enter the file.

For swarch, the file resembles this:

```
Clli Dpc Eqtype Stp Owner Hnpa Ai Ccd

   Ipaddress Description

sv009099009;-;4ess;sv02;svtst;508; on;-; -;switch

svaxetrado2;-;axe10;-; svtst;-;on; -;-;switch
```

5 Change the second line to represent the element you are adding, and save the file.

Important! For entities monitored by GeoProbe, you must populate the Dpc field to identify DEs.

Reference: For what to put in each field of the swarch table, see "swarch Table" (p. A-156) (or another "arch" table's entry in that appendix).

6 To insert the record from the temp file into the swarch table, enter

```
dbedit -i -t swarch -f temp -s";"
```

7 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see "Correct dbedit Errors" (p. 3-27) .

8 Verify the CLLI is in swarch.

Example:

If CLLI is 22222222222 enter:

```
sui find source=swarch search=clli=22222222222
```

9 Remove the temp file.

10 Does the record you added to Swarch or another "arch" table have an STP in its Stp field?

- If no (value is "-'), go to the next step.
- If yes, ensure the STP is defined in the Stparch table. If it is not, add it to Stparch.

  Example: You see sv01 in the Stp field of the RE's record in swarch.To see if STP sv01 is in scparch, enter: `sui find source=scparch search=stp=sv01`

  Reference: For how to edit tables, see "dbedit Insert or Update Example" (p. 3-32) . For how to populate stparch fields, see "stparch Table" (p. A-155) .

11 If the RE's record in Swarch has Eqtype of 4ESS, or DMS100, DMS200, etc., ensure the RE's SCPs are in the Scparch table. If they are not, add them. (This table tells NTP how to correctly fill in CFIM's Rs an Ds fields.)

END OF STEPS

Add an entity to rearch

Purpose

For an entity to be an RE (on a CFIM), it must be in the rearch table.

Reference: To edit files in this procedure you can use any ASCII text editor, such as *vi* . For more information on using *vi* , see "Edit (vi) ASCII Files" (p. 3-13) .

Procedure

Use this procedure to add an entity to the rearch table.

1 Enter **sui find source=swarch** and look in the output's Clli field for the CLLI of the new RE. Is it there?

- If yes, go to the next step.
- If no, STOP. You must add the RE to the swarch table (see "Add to Swarch (or other "arch") Table" (p. 4-61)). Then return here.

2 To make a template record for the rearch table, enter

```
sui find source=rearch search=conv=type noheader delim='";"'
maxsave=1 > temp
```

Reference: For converter types (conv field), see the Conv field in the rearch table, on "rearch Table" (p. A-129) .

Example: For any RE type using the configurable converter, enter

```
sui find source=rearch search=conv=ccc noheader delim='";"'
maxsave=1 > temp
```

3 Use a text editor (such as *vi*) to edit the temp file.

Response

The file resembles this:

```
#re;Source;Tag;Conv;Down;Degraded;Interval;Calc
svaxetrado1; trado;2 -; univ; 0; 3; 100 y; 100; est5edt
```

Important! For 4ESS switches, the tag field must have an entry OTHER than "-".

4 Change the second line to represent the switch you are adding, and save the file.

Important! For 4ESS switches, associate the tag (see the previous step) with the channel assigned from the CP database.

Reference: For what to put in each field, see “rearch Table” (p. A-129) .

5 To insert the record from the temp file into rearch, enter
`dbedit -i -t rearch -f temp -s";"`

6 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see “Correct dbedit Errors” (p. 3-27) .

7 To verify the CLLI is now in rearch, enter (this example uses CLLI 22222222222):

`sui find source=rearch search=re=22222222222`

8 Remove the temp file.

9 Use “Manage Network Groups and Segments” (p. 7-30) to add the RE to network groups or segments, as desired.

END OF STEPS

Map an RE to its Swarch DEs

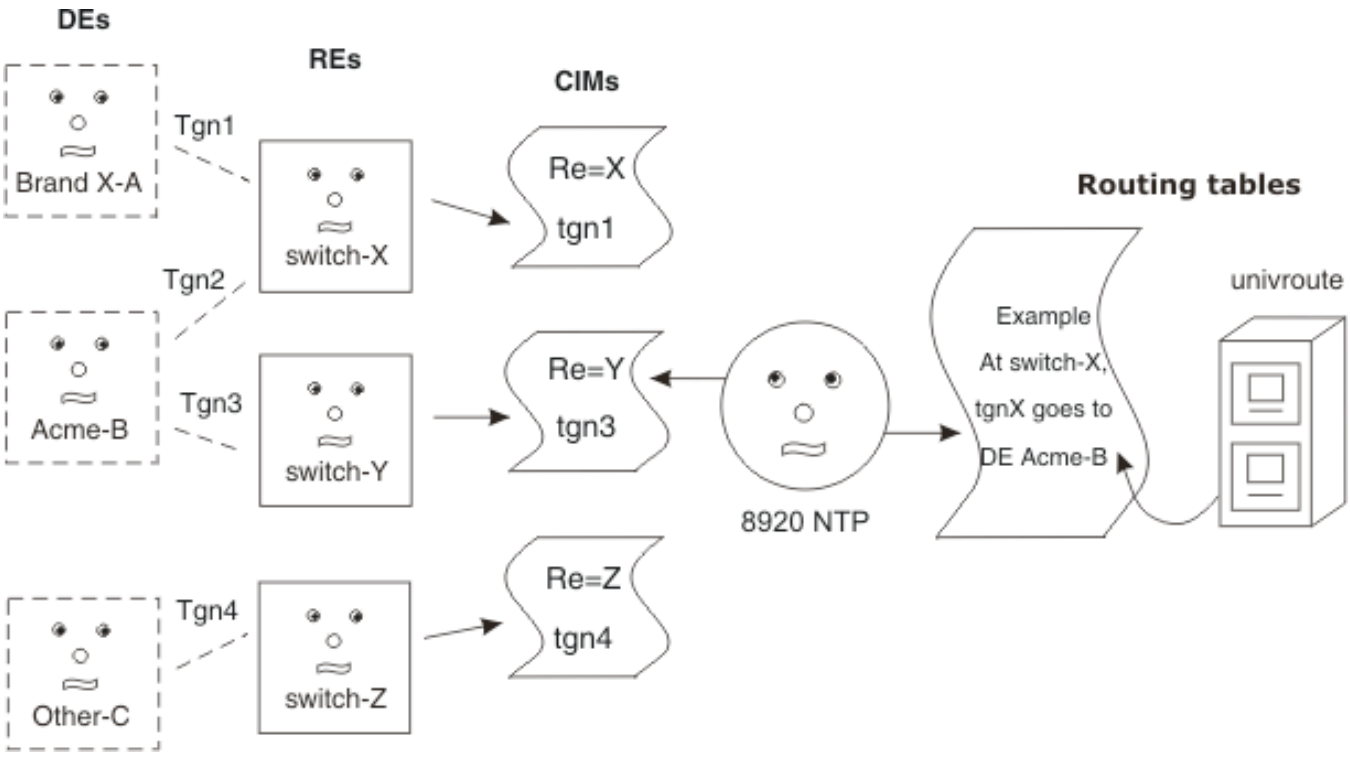
Purpose

This section gives a procedure for mapping an RE to its DEs, if those DEs are found in the swarch table. This includes trunk routing, cell routing, and gateways (non-digit lookup).

Important! Routing tables are not always used. See "Map an RE to its swarch DEs" (p. 4-68).

What are routing tables

This illustrates how most routing tables are used.



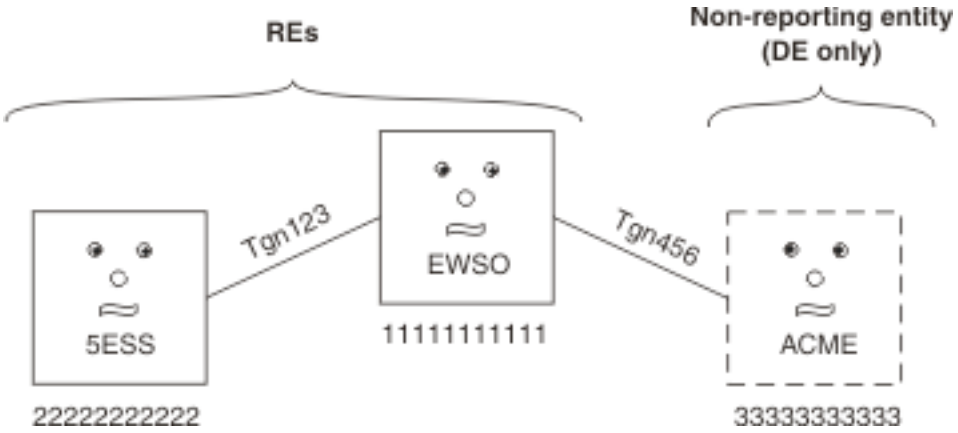
In detail:

- *REs*. NTP knows REs by looking at the CFIMs.
- *DEs*. NTP knows DEs by taking a Tgn, tgclli, or cell number from the CFIM and looking it up in the RE's routing table.
- *Related*. The related entity is determined if another network element is used in setting up and processing the call, for example an SCP, tandem, or gateway. NTP may derive the related entity from a routing table, and put it in the CFIM's Related field. You need do nothing special for Related's.

Example

Since REs may see each other as DEs, you may need to use this procedures multiple times, from the viewpoint of each RE.

For example, to define the configuration in the illustration.



From the viewpoint of this RE	Update this routing table	With this Clli:Tgn;DE
11111111111	ewsdroute	11111111111;123;22222222222 11111111111;456;33333333333
22222222222	route5e	22222222222;123;11111111111
33333333333	Not applicable. Not an RE.	

Map an RE to its swarch DEs

Purpose

Use this procedure to map an RE to its DEs found in swarch, so the REs' CFIMs will correctly populate the DE field.

Reference: To edit files in this procedure you can use any ASCII text editor, such as **vi**.

Procedure

Use this procedure to map an RE to its DEs found in swarch.

1 Use this procedure ONLY if DE is in swarch. For other DEs, such as an SCPs (in scparch) start at "Add DE-Only Elements" (p. 4-31). Do NOT use this procedure for cell base stations (although they are in swarch). Instead use "Add a cell base station" (p. 4-42), which maps REs to DEs in cellroute.

2 See the second column, below, for what routing table to dbedit. If there is an NA in the second column it means no route table is used—so SKIP this procedure, and do what the column says.

If RE is from conversion:	Map the RE to its DEs in this routing table...
1AESS	route1a
4ESS	NA. Do nothing. DEs are determined from data in CIMs.
5ESS or 7R/E PLS	route5e
AUTOPLEX MSC	route5e
DMS MTX MSC	dmsroute
OTR (5ESS osps module)	NA. *dbedit* lrn2ne, gtspec, and potsroute.
OTR (DMS tops module)	NA. *dbedit* lrn2ne, gtspec, and potsroute. For TOPS LNP, also *dbedit* dmsroute.
DMS	dmsroute
EWSD	ewsdroute
S1240	s1240route
Succession SN05 and SN06	dmsroute

If RE is from conversion:	Map the RE to its DEs in this routing table...
GeoProbe	NA. If a DE has a point code, make sure it is populated in the dpc field of the DE's swarch record, and in the pc2clli table, if applicable.
AXE 10	NA. Ensure each DE, and RE, is in the id2ne table. (This RE sees only its own Retype as DE's.)
AXE 10 TRADO	univroute
Lucent Softswitch	univroute
IPDRs	NA. Ensure DEs have ipaddress in their swarch records.

3 Make sure the to-be-mapped DEs are in swarch (if needed, use "Add to Swarch (or other "arch") Table" (p. 4-61)).

4 Find out each Tgn and far-end CLLI out of the RE.

5 In the chosen table (from Step 2 of this procedure), use **dbedit** to add a record for each Tgn-DE pair (from Step 4 of this procedure). To start, make a template record for the appropriate route table.

Example: For the any route table, enter the following, where *routetable* is the table name.

```
sui find source=routetable noheader delim='";"' maxsave=1 >
temp
```

6 Use a text editor (such as **vi**) to open the temp file.

7 Change the second line to represent the switch you are adding as a distant switch, add additional lines for other DEs, and save the file.

8 Insert the record from the temp file into the routing table.

Example: For ewsdroute, enter

```
dbedit  -i -t ewsdroute -f temp -s";"
```

9 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see “Correct dbedit Errors” (p. 3-27).

10 Verify the record or records are added.

Example: To verify CLLI 11111111111 is in ewsdroute, enter

```
sui find source=ewsdroute search=clli=11111111111
```

11 Remove the temp file.

END OF STEPS

Define Routes to Eliminate "?"s

Question marks"

You sometimes see "?" in an output field. Typically, this means you need to put a missing value in a reference database.

Important! Two other null characters ("-" and "~") are okay, with the exception of the rt field for 4ESS. See “Null characters” (p. 3-8).

How to fix "?"

Only some fields may display a "?". Those fields are listed in the following table, with references for how to eliminate the "?".

If you see "?" in this field...	On this output...	Go to...
Lrne	• Find CFIM • Trapcfim	“Eliminate "?" in lrne” (p. 4-73)
DE	• Find CFIM • Trapcfim	“Eliminate a "?" DE” (p. 4-75)
Ne	• Ascreen when Type is DE • Trapalert when Type is DE	
Dpc	• Find CFIM	The DCP can be used to determine the DE.

Eliminate "?" in Lrne

"?" in the lrne field

If you see "?" in the lrne (location routing number network element) field of Find CFIM or Trapcfim output, you need to put an entity in the lrn2ne table.

Important! If the lrn2ne table is missing LRN information, then the LRNE field will be populated with a "-".

Note

- LRNE is part of the LNP feature. LNP is separately optional for different entity types.
- Other than keeping the Lrn2ne table updated, there is no other housekeeping for you to do for the LNP feature. If this table is out of date, the LRNE field will be incorrect or will say "?". Nothing else is affected.
- To see what is currently in the lrn2ne table, use **`sui find`** to create a temporary file that you can view (or edit). Enter **`sui find source=lrn2ne > temp`**

Reference: See “lrn2ne Table” (p. A-92).

Eliminate "?" in lrne

Procedure

Use this procedure if you see a "?" in the Lrne field of Find CFIM or Trapcfim output.
Reference: Examples in this procedure use the **vi** editor. For more information on using **vi** , see "Edit (vi) ASCII Files" (p. 3-13) .

1 On Find CFIM or Trapcfim output, write down the LRNs from records where LRNE is "?".

Example: On Find CFIM Output, you find all CFIMs with LRNE of "?" have LRNs of either 614123456 or 61411111. You would write down those two LRNs.

2 From switching, translations, or other persons, find out the network element that each LRN maps to, and write that beside each LRN you wrote down.

3 Use a text editor (such as vi) to open a new temp file.

4 In the file, type in a line for each LRN you are adding, and then save the file. (If you want, you can type in a header line for reference, as long as you make sure you start it with #.)

Example: The header line and lines for two Lrns would resemble the following:

```
#Lrn;Ne
614123456;cmbsohbrhx1
614111111;chgsilabcx2
```

Reference: For what goes in each field, see "lrn2ne Table" (p. A-92) .

5 To insert the records from the temp file into the lrn2ne database, enter

dbedit -i -t lrn2ne -f temp -s";"

6 Did you receive a messages ending with: "Errors saved in file..."?

- If NO, go to the next step.
- If YES, see "Correct dbedit errors" (p. 3-30) .

7 Use **sui find** to verify that your update is in the lrn2ne table.

Example: Enter **sui find source=lrn2ne > temp2**

Then **vi** or **cat** the temp2 file. When you are done, to remove the file, enter **rm temp2**

8 Remove the temp file.

END OF STEPS

Eliminate a "?" DE

Procedure

The procedure to administer NTP to eliminate a "?" DE depends on the RE and conversion type. Some effort in analysis is necessary.

First determine the Retype by viewing the rearch table. Based on the general RE type, the key areas that require attention differ.

RE conversion type	Use these guidelines...
Circuit-based conversions (TGN-based routing)	For circuit-based REs, use Compute or viewcfim to see the RE and TGN. Then **dbedit** the appropriate routing table, such as univroute, routet5e, dmsroute, ewsdroute, etc.
Cellular conversions (cell number-based routing)	For cellular REs, look at the CIM for the cell number and use it to dbedit the *cellroute* table (cell field).
IPDR conversions (gateway IP address-based routing)	For IPDR REs, look at the CIM for the IP address of the gateway, and use it to **dbedit** the swarch table (ipaddress field).
Digits (no TGN or gateway, using SS7)	For digit-based REs, use Compute to see the RE and digits. Then **dbedit** the appropriate table, such as scproute or gtspec.
DPC (no TGN, gateway, or digits)	These cases are rare. For DPC REs, look at the CIM for the destination point code, and use it to **dbedit** the swarch table.

FDCs

Overview

When NTP translates a CIM to a CFIM, it adds an FDC (final disposition code) to categorize the CFIM, typically for thresholding.

When to add or modify an FDC

Add or modify FDCs in the following circumstances:

- When you add a new conversion. In this case, you will typically have help from your NTP support organization since you will probably be adding many FDCs.
- If you see a discarded CIM in the incon, univlog, and sccs logs because NTP cannot determine an FDC for a CIM (see "incon Log" (p. 10-29) , "univlog Log" (p. 10-37) , and "sccs Log" (p. 10-35)). This happens when an RE sends a new message type.
- To broaden or narrow what an FDC means. (see "Broaden or narrow an FDC" (p. 4-76)).

Broaden or narrow an FDC

With some conversions, FDCs are defined one-to-one with a code on the CIM. (For example, 4ESS conversion takes a CIM's FHC and maps it to an FDC in the fdc table.) These one-to-one FDCs cannot be broadened or narrowed. But some conversions take more than one CIM string to map to an FDC, using both the FDC table, and another table, such as acode2fdc. With these conversions, one or more strings in (for example) acode2fdc can be mapped to one or more FDCs in the fdc table, enabling you to broaden or narrow the FDC. (See "Add or modify an FDC" (p. 4-78)).

Example: From a DMS switch, CIMs with code TRK121 can mean different problems, each identified by a reason or "TRBCODE" (such as NO_START_DIAL shown here).

```
45 TRK 121 2472 FLT OUTPULSING TRBL CKT NYCNNY94001DE 1

 TRBCODE NO_START_DIAL TRBLINFO

 NIL

 FAILURE FIRST_TRIAL_FAILURE

 INCTRK CKT NYCMNY72BK1 33 CLDNO 3734772

 DIGSOUT $ CALLID 244328 NILC
```

Here are records in the acode2fdc table mapping TRK121 messages to separate FDCs by trouble code. (FDCs must be defined in the fdc table.)

```
Acode                   Fname       FDC

NO_START_DIAL           trk121      nsd121

UNEXPECTED_STOP_DIAL    trk121      nsd122

REVERSED_TRUNK          trk121      rt121
```

Add or modify an FDC

Procedure

Use this procedure to add or modify an FDC name. *Reference:* Examples in this procedure use the **vi** editor. For more information on using **vi** , see "Edit (vi) ASCII Files" (p. 3-13) .

1 Identify the conversion used for the FDC's CFIMs.

Reference: See "Find a CFIM's conversion" (p. 4-11) .

2 Go to the FDC table (see "fdc Table" (p. A-68)) and write down the value you will assign to each field.

Important! For 4ESS and 5ESS MDIIs, the FDC name must match the switch final disposition code (failure or event). For other switches, you can select the FDC name. You may need to consult switch references, as well as feature design documents supplied by your NTP support organization.

3 See if the value you wrote down for the:

- eqtype field is found in the type field of the eqtype table
- sig field is found in the type field of the signaling table
- st field is found in the type field of the st table

Example: To verify a value *xyz* is in the eqtype table, enter
sui find source=eqtype search=type=xyz

4 Were each of the values above found?

- If YES, go to the next step.
- If NO, add the missing value to the eqtype, signaling, or st table.

Reference: For the general procedure for adding values to tables, see "dbedit Insert or Update Example" (p. 3-32) .

5 Make a backup ASCII file of the FDC table, in case you later need to back out of your changes.

To do this, enter **sui find source=fdc noheader delim=' ";" ' > hold_fdc**

6 Copy the header and first record into from the fdc database into a temp file.

To do this, enter
sui find source=fdc noheader delim=' ";" ' maxsave=1 > temp

7 Use a text editor (such as **vi**) to open the temp file.

Response

The file holds two lines, resembling this:

```
#Fdc;Tc;Eqtype;Al;S;D;Sig;St;Tm;Ai;Mc

100p_1;dms;dms100;mi;n;o;-;-;p;on;-
```

8 Change the second line of the temp file to the values you wrote down in Step 2 of this procedure and save the file.

Important! In the Ai field, enter **off** .

9 To add the record to the fdc table, enter **dbedit -i -t fdc -f temp -s";"**

10 Did you receive a messages ending with: "Errors saved in file..."?

- If NO, go to the next step.
- If YES, use the procedure in "Correct dbedit Errors" (p. 3-27) .

11 Verify the FDC is in the fdc table.

Example: To verify an FDC named *xyz* is in the fdc table, enter
sui find source=fdc search=fdc=xyz

(If you get no response, the FDC is not there.)

12 Recommended: add help text for the new FDC. For the procedure, see "Manage Help Texts" (p. 9-18) .

13 Further map the FDC in the appropriate table, as shown below.

If the FDC is for this conversion:	Further map the FDC as follows:
1AESS	ess1a2fdc
4ESS	(none besides the fdc table)
5ESS MDII	(none besides the fdc table)
5ESS DSE	acode2fdc
5ESS ASSERT	assert2fdc (also see "Delete an FDC" (p. 4-82))
7R/E PLS	acode2fdc (also see "7R/E PLS FDCs" (p. 4-85))
AUTOPLEX MSC, PCMD, EvDO PCMD, EvDO CP FAIL	acode2fdc
DMS-MTX MSC	acode2fdc (also, see "DMS MTX FDCs" (p. 4-87))
DMS-MTX Number Portability (NP)	See "DMS MTX NP" (p. 4-88) .
DMS MSC	acode2fdc (also, see "DMS MSC FDCs" (p. 4-89))
OTR	otr2fdc (see "OTR FDCs" (p. 4-90))
DMS	acode2fdc
DMS DFIL	acode2fdc (also, see "DMS DFIL FDCs" (p. 4-86))
EWSD	acode2fdc
S1240	acode2fdc
Succession SN05 and SN06	acode2fdc
GeoProbe	See "GeoProbe FDCs" (p. 4-93) .
AXE 10	(none besides the fdc table)
AXE 10 TRADO	acoded2fdc, dcode2d, scode2sig, stcode2st (see also "CDR FDCs" (p. 4-96))
Lucent Softswitch	None besides the fdc table (see also "CDR FDCs" (p. 4-96))
IPDRs	acode2fdc (see also "CDR FDCs" (p. 4-96))
Any consultant added	Consult your NTP support organization (see also "CDR FDCs" (p. 4-96))

END OF STEPS

Delete an FDC

Procedure

Use this procedure to delete an FDC. *Reference:* Examples in this procedure use the **vi** editor. For more information on using **vi** , see "Edit (vi) ASCII Files" (p. 3-13) .

1 View the FDC table (see "fdc Table" (p. A-68)) and identify the FDC to be deleted.

2 Use **mod_helptext**delete the help text for the FDC. For the procedure, see "Manage Help Texts" (p. 9-18) .

3 Use the table found in "Add or modify an FDC" (p. 4-78) to determine if, based on the conversion, the FDC was mapped to any additional tables.

- If yes - continue with the next step
- If no - continue with Step 8.

4 Use **dbedit** to remove the FDC from any additional tables to which it was mapped.

5 Copy the header and record for the FDC you wish to delete into a temp file.

To do this, enter

```
sui find source=fdc se=fdc=<FDC_to_delete> noheader delim=' ";"
' > <temp_file>
```

6 Use a text editor (such as **vi**) to open the *<temp_file>* file.

Result: The file holds two lines, resembling this:

```
#Fdc;Tc;Eqtype;Al;S;D;Sig;St;Tm;Ai;Mc
100p_1;dms;dms100;mi;n;o;-;-;p;on;-
```

7 Verify that the FDC shown in the *<temp_file>* is the FDC is the one you wish to delete.

8 To delete the record in the fdc table, enter

```
dbedit -d -t fdc -f <temp_file> -s";"
```

9 View the FDC table (see “fdc Table” (p. A-68)) and verify that the FDC was deleted.

END OF STEPS

5ESS Assert FDCs

Purpose

This section contains information that may be useful when defining FDCs for 5ESS Assert messages.

The **assert2fdc** table contains the assert code to fdc translations for 5ESS Assert messages (see "assert2fdc Table" (p. A-21)). It is used to determine the fdc for the assert. The error codes for the asserts may change from release to release. Therefore, this table may need to be updated when the 5ESS switch is upgraded.

Mapping 5ESS Asserts to FDCs

To update the assert2fdc table, edit (**dbedit**) the table as follows:

- *ErrorCode* — Either
  - Assert error code number (e.g., 30035)
  - or error type string (e.g., RDSTATIC_DATA)
- *Release* — 5ESS release number (e.g., 5E16.1).
  Note
  For RTA-DCF asserts, the release should be 5e.
- *AssertType* Type of assert (e.g., Rept_manual or Rept_rta_dcf).
- *FDC* — FDC of the assert (e.g., Rtdb)
- *TrbReason* — mnemonic for the manual assert (e.g., CMHOPCNT). This is found in the 5ESS documentation.

Example

The following is an example of the assert2fdc table.

```
Error    Code   Release        Asserttype  FDC  Trbreason

30035    5E17.1 report_manual  Hopovfl     CBEXCHRTG

30035    5E16.2 report_manual  Hopovfl     CCBEXCHRTG

29835    5E16.1 report_manual  Hopovfl     CCBEXCHRTG

etypenul 5e     report_rta_dfc rtsftw      -
```

7R/E PLS FDCs

Purpose

This section gives information that may be useful when defining FDCs for 7R/E PLS (Packet Local Solution) CFIMs. Most 7R/E PLS FDCs are 5ESS FDCs, defined in Fdc and Acode2fdc tables.

Important! Some 7R/E PLS FDCs may be appropriate for system day alerting, if you use it.

7R/E PLS CFIMs

NTP converts the following 7R/E PLS CIMs to CFIMs:

- Existing circuit-side 5ESS MDIIs based on ISUP signaling.
- A subset of existing 5ESS MDIIs based on BICC signaling.
- Three new MDIIs for packet-side failures of the 7R/E PLS 3.0.
  - ATMRJ — The Terminating Packet switch (TPS) encounters an IPDC signaling failure with the Interworking Gateway (IWG, formally called PVG) for one of the following reasons.
  - RELEASE COMPLETE message received
  - Timeout waiting for UNI message
  - AEVENT — The Originating Packet Switch (OPS) or TPS gets an EVENT message for one of the following reasons.
  - Timeout waiting for STATUS message
  - Call state mismatch on STATUS ENQUIRY procedure
  - UNI timer expired
  - AOMRJ — The OPS receives a failure from an IWG that encountered a timeout during UNI signaling or other unexpected events.

New 7R/E PLS FDCs

There are a number of new 7R/E PLS FDCs starting with these strings:

- atmrj
- aevrst
- aomrj

For more information, see these strings in the Fdc and Acode2fdc tables.

DMS DFIL FDCs

Purpose

This section contains information that may be useful when defining FDCs for DMS DFIL messages.

DMS DFIL (Data Fill) is a type of log message. Most DFIL messages (message numbers) are contained in the acode2fdc table by default and are mapped to an appropriate FDC (see "acode2fdc Table" (p. A-9)). Any message number not contained in the acode2fdc table must be manually added and mapped to an FDC.

FDCs for DMS DFIL messages are defined in the Fdc and Acode2fdc tables.

Mapping DMS DFIL to FDCs

DMS DFIL messages contain a DFIL number (the string "DFIL" with a 3 digit numeric code) and the date and time of the log.

An example of a DFIL100 log message is as follows:

*DFIL100 JAN01 09:21:03 XXXX FAIL TRANSLATION ERROR HOST 00 1 04 19 DN 9097224112 OG CKT = TOPOGNY 1, CALLED DR = 90114466062112345 PREFIX DR = $, SUFFIX DR = 0114466062112345 MORE THAN 15 DIGITS IN 1 STAGE OF OUTPULSING

To add a DFIL message number to the acode2fdc table and map it to an appropriate FDC, populate (**`dbedit`**) the acode2fdc table as follows:

- **`acode`** — Enter the DFIL number (e.g., DFIL100).
- **`fname`** — Enter "~".
- **`fdc`** — Enter the FDC to which you want to map this DFIL message number (e.g., Trans, Config, etc.). You can map to an existing FDC or create a new FDC. New FDCs must be added to the fdc table (see"fdc Table" (p. A-68)).
- **`Error origin`** — Enter "-" (blank).

Example

The following is an example of the acode2fdc table.

```
Acode   FnameFdc  Error Origin
DFIL100 ~  Trans  -
DFIL103 ~  Trans  -
DFIL104 ~  Trans  -
```

DMS MTX FDCs

Purpose

DMS MTX is the wireless DMS switch. This section contains information that may be useful when defining FDCs for DMS MTX switches.

FDCs for DMS MSC switches (and for regular wireless DMS switches) are defined in the Fdc and Acode2fdc tables.

DMS MTX FDCs

For log messages C7UPXXX, TRKXXX, LNPXXX and TCPXXX, the DMS MTX switches use the same FDC definitions used for regular (wireless) DMS switches.

But, you must define new FDCs for the following log messages:

- **CELL1XX** for failed calls. (CELL2XX for test, CELL3XX for manual, and CELL9XX probably are not useful.)
- **CLFLXXX** for failed calls.
- **DROPXXX** for dropped calls.

Populate (**dbedit**) the acode2fdc table as follows:

- **acode** — A code from one of these LOG fields: TRBL, TRBLCODE, INFO ATD, REASON, EVENT, or "EVENT:". (Labels may use a "=" or ":".)
- **fname** — The log name, such as CELL100, CLFL100, or DROP100.
- **fdc** — The name you want to give the final disposition code based on acode and fname.

DMS MTX NP

Purpose

DMS MTX Number Portability (NP) is a log produced by the DMS MTX switch.

FDCs for DMS MTX NP logs are defined in the Fdc table.

NP FDCs

You define FDCs for the following log message:

- **NPXXX** for number portability.

Populate (**dbedit**) following fields in the fdc table as follows:

- **fdc** — The name you want to give the final disposition code.
- **tc** — The trouble category (tc) of the FDC.
- **eqtype** — Indicates the equipment type that generates this fdc.

The following shows an example of an entry for the NP log in the fdc table:

```
Fdc     Tc     Eqtype    Al S D Sig    St   Tm Ai  Mc
np101   lnp    dms-mtx   mi f i isup   -    p  on  n
```

DMS MSC FDCs

Purpose

DMS MSC (Mobile Switching Center) is a wireless DMS switch. This section contains information that may be useful when defining FDCs for DMS MSC switches.

FDCs for DMS MSC switches (and for regular wireless DMS switches) are defined in the Fdc and Acode2fdc tables.

DMS MSC FDCs

For log messages C7UPXXX, TRKXXX, LNPXXX and TCPXXX, the DMS MSC switches use the same FDC definitions used for regular (wireless) DMS switches.

But, you must define new FDCs for the following log messages:

- **GBSSXX** for Base Station Subsystem.
- **GBCSXXX** for Base Station Controller.
- **GINXXX** for Intelligent Network.
- **GMSCXXX** for Mobile Switching Center.

Populate (**dbedit**) the acode2fdc table as follows:

- **fname** — logname such as GBSS300, GBCS300, GIN300, or GMSC601.
- **acode** — code from the TREATMENT, DESCRIPTION, or TROUBLE fields. If these are not present, the log name may be used.
- **fdc** — The name you want to give the final disposition code based on acode and fname.

OTR FDCs

OTR comparison

OTR (operator trouble reports) CFIMs are from reports entered manually by operators. NTP collects them from either:

- 5ESS OSPS (Operator Services Position Systems) module.
- DMS TOPS (Traffic Operator Position Systems) module.

Save OTR CFIMs to the OTR table

Overview

To ensure OTR CFIMs go to the OTR summary table (where they are retained much longer than regular CFIMs), ensure OTR CFIMs' FDCs are in the otr2fdc table. If an FDC is missing, **dbedit** to add it.

System day

System day thresholding enables you to replace normal 5-minute and hourly thresholds with daily thresholds. This is ideal for CFIMs that trickle in slowly, such as OTR CFIMs. See "System Day Thresholding" (p. 8-43).

OTR fields you can affect

Use this table to affect OTR CFIMs, **dbedit** the otr2fdc, fdc, or potsroute tables.

This field...	Gets its value from these reference database tables...
FDC	A lookup into the otr2fdc table, which maps the CIM OTR trouble codes to FDCs. The FDC must also be defined in the fdc table. The otr2fdc table contains the following fields. • TRB -- This field contains the actual value of the trouble code field in the OTR. This is a key field in the otr2fdc table. • FDC --This field contains the FDC indicated by the trouble code.This value must exist in the fdc field of the fdc table. • OC -- This field indicates whether an operator or customer encountered the problem, as indicated by the trouble code.Valid values for this field are: c (customer encountered) and o (operator encountered).
RE	Either: • For operator-encountered OTRs (determined by the OC field of the otr2fdc database table), the RE is the reporting OSPS/TOPS. • For customer-encountered OTRs, the RE is obtained by doing a lookup into the potsroute table using the calling party digits as the key. If this lookup fails, then the RE is determined by doing a lookup into route5e or dmsroute using the trunk group information in OTR. If this lookup also fails, the RE is set to ? (unknown).
DE	A lookup into either using the called digits from the CIM as the key: • The gtspec table. • The potsroute table.

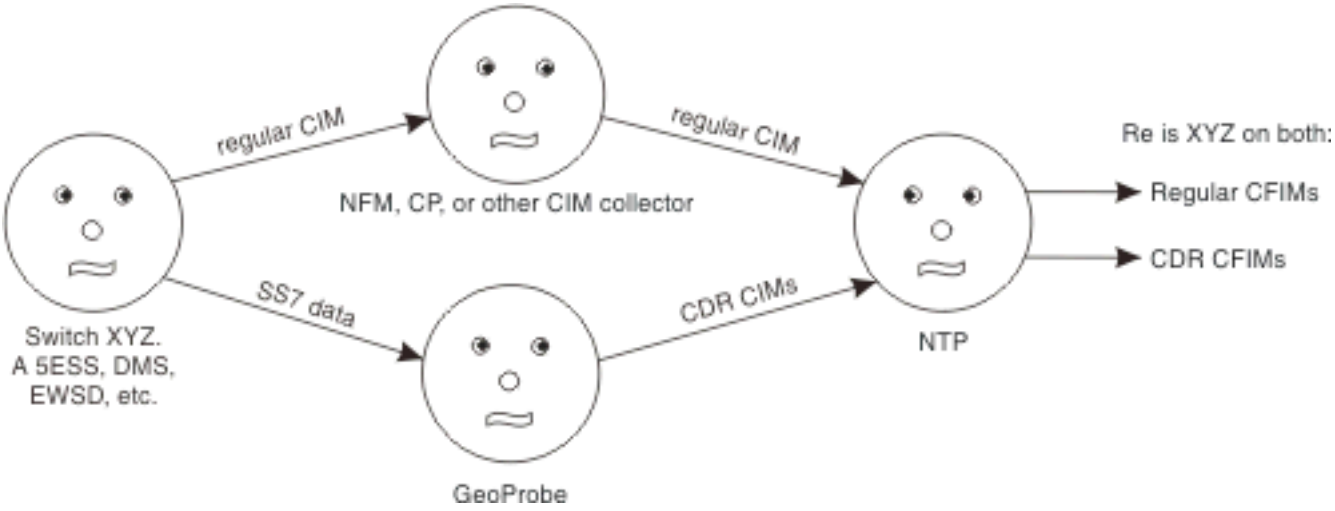
This field...	Gets its value from these reference database tables...
Related entity	Either: • For operator-encountered OTRs the Related Entity is obtained by doing a lookup into the potsroute table using the calling party digits as the key. If this lookup fails, then the Related Entity is determined by doing a lookup into route5e or dmsroute using the trunk group information in OTR. If this lookup also fails, the Related Entity is set to ? (unknown). • For customer-encountered OTRs, the Related Entity is the reporting OSPS/TOPS.

GeoProbe FDCs

Background

GeoProbe conversion enables NTP to convert GeoProbe CDR CIMs to CFIMs. GeoProbe is a mediation system, monitoring SS7networks. For NTP, it is a "source", supplying CDR CIMs.

This illustrates that you may see an RE from one conversion (such as the 5ESS conversion), and then again, from the GeoProbe conversion.



Note

- SS7 data comes, NOT from switches, but from probes between switches and STPs.
- Currently the CDRs GeoProbe sends to NTP are limited to those reporting SS7 data about call failures.
- GeoProbe CIMs arrive at NTP in binary code. NTP reformats them into what it displays as GeoProbe CIMs, before reformatting them into GeoProbe CFIMs.

When to add a GeoProbe FDC

If the incon log reports it is unable to assign an FDC to a CFIM (where the CFIM source is a GeoProbe, such as inet), it means the CFIM had a caus code not in acode2fdc.

Reference: Also see "When to add or modify an FDC" (p. 4-76).

GeoProbe FDC fields

In this procedure, the following assignments are recommended:

- fdc— Unique, up to 7 characters. Use the model of other SS7 FDCs, and name it in the range ccs1 to ccs127, where the number is the caus code.
- tc — suggested values by caus code:
  - nrlevt — Normal event. If caus code is 1-31.
  - rscunv — Resources unavailable. If caus code is 34-47.
  - srvunv — Service or option unavailable. If caus code is 50-63.
  - srvnim — Service or option not implemented. If caus code 65-79.
  - invmsgI — Invalid message. If caus code is 87-95.
  - ptlerr — Protocol error. If caus code is 97-111.
  - itwcls — Interworking class. If cause code is 127.
- eqtype — "-". Field is ignored.
- al — Either Cr (critical), Ma (major), or Mi (minor).
- s — "f" fatal.
- d — "-". Field is ignored.
- sig — "ccitt7".
- st — "-". Field is ignored.
- tm — "p", meaning standard thresholding.
- ai — "off" for now.

Add a GeoProbe FDC

Procedure

Use this procedure to add or modify a GeoProbe FDC.

1 Find the caus code that is not yet in the Acode2fdc table.

2 Add the new FDC to the Fdc table

Reference:

- For field values to assign, see "GeoProbe FDC fields" (p. 4-94).
- For the general procedure for adding values to tables, see "dbedit Insert or Update Example" (p. 3-32).

3 Recommended: add help text for the new FDC. For the procedure, see "Manage Help Texts" (p. 9-18).

4 Add a record to the acode2fdc table, where fields are:

- acode — caus code from the new FDC's CIM.
- fname — "SS7".
- fdc — same fdc as in Step 2.

Reference: For the general procedure for adding values to tables, see "dbedit Insert or Update Example" (p. 3-32).

END OF STEPS

CDR FDCs

Purpose

For any of the following conversions, if the icon log reports it is unable to assign an FDC to a CFIM, it means the CFIM had a caus code not in acode2fdc.

- AXE 10 TRADO
- Lucent Softswitch
- IPDRs
- Any consultant added.

  Important! The source type on the CFIM will be "ccc".

When to add a CDR FDC

Add a CDR FDC if necessary to reprocess CDRs that appear in the reprocess directory for a CDR source.

Reference: See the following sections for more information:

"Assign or Modify FDC Group and Network Group/Segments for BB-GUI Users" (p. 7-28)

"When to add or modify an FDC" (p. 4-76)

CDR FDC fields

The following assignments are recommended:

- fdc— Unique, up to 7 characters. With CDR type CFIMs, FDCs are:
  - inprog — successful call in process. These are not counted in alert cases or summary reports (if your system implements additional traffic analysis).
  - comp — completed call
  - busy — called party line is busy (cause code 17)
  - net_fail — network, switching, or signaling failure (cause codes 4, 8, 9, 18, 27, 29, 31, 34, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 49, 50, 51, 53, 54, 55, 57, 58, 62, 63, 65, 66, 69, 70, 79, 87, 88, 90, 91, 95, 97, 99, 102, 103, 110, 111, 127, 255)
  - no_ans — calling party disconnects the call prior to answer (cause codes 16, 19)
  - route_fail — call routing failure (cause codes 1, 2, 3, 5, 6, 20, 21, 22, 24, 25, 26, 28)
- tc — Either:
  - ok — If Fdc is comp, busy, no_ans, or call_ab
  - inprog — If Fdc is inprog
- eqtype — cdr

- al — Either Cr (critical), Ma (major), or Mi (minor).
- s — "f" fatal.
- d — "-". Field is ignored.
- sig — "ccitt7".
- st — Typical values, cellular, voice over IP, toll, local POTS, international, incoming international. (This may be populated directly from the CDR or by other means, such as through the “gtspec Table” (p. A-77) or by using the “stcode2st Table” (p. A-153).)
- table tm — "p", meaning basic thresholding.

Add Motorola iDEN Count

Overview

The iDEN Support feature provides support for Performance Count records received from the Motorola's iDEN equipment. These counts document air side failures due to traffic or equipment problems. The counts are provided in the mediation system every 30 minutes on a sector basis.

8920 NTP collects these counts via a file-based interface with the mediation system, and converts each individual count into a CFIM database record. The **`count`** value is populated in the **`weight`** field, which provides the actual number of calls represented by the record. Alerting is done on the value of the **`weight`** field, and notifies the analysts when a count deviates from the norm by a statistically significant amount.

The feature supports a basic set of counts as follows:

- NTRA_CELL_HO_REQ
- INTRA_CELL_HO_FAIL
- INTRA_CELL_HO_LOSTMS
- BSC_SWITCH_FAILURE
- INTRA_BSC_HO_FAIL
- INTRA_BSC_HO_LOSTMS
- INTER_BSC_MS_FAIL
- HO_REQ_MSC_FAIL
- CONN_REFUSED
- UNSUCCESSFUL_ASSIGNMENT
- SUBRATE_BLOCKING_FIRST_ATTEMPT

All other counts provided on the mediation system can be added to the interface by the addition of records to the 8920 NTP reference database.

Purpose

Use the following procedure to add Motorola iDEN counts to the 8920 NTP reference database.

Procedure

1 Log on the 8920 NTP host as **`ntp`**.

2 Determine which count is to be added, and decide on an associated **fdc** (7 characters or less).

3 Add this fdc to the **fdc** table, filling in the other fields as appropriate. Counts that do not indicate a call drop or failure should be given a status (**s** field) of "**n**" (non-fatal).

4 Add the fdc and count name to the **acode2fdc** table. The count name is entered in the **acode** field. The **fname** is **iden_count**.

5 Add the count to the **count_def** table. The **source** and **conv** fields are taken from the **rearch** table for the **re** associated with this count. The position field is populated with the field number of the count. The **name** field is populated with the count name.

END OF STEPS

Delete a Network Element

Procedure

To delete a network element, use the procedure in this chapter that you followed to add the element, but in reverse order.

The system prompts you if you attempt to remove an element from a reference database table where there are field dependencies to other tables.

Reference: For information on various database field dependencies, see "Field Dependencies" (p. 3-38), "Field Dependency During Installation" (p. 3-43), and information on the various database tables in Appendix A, "Reference Database Tables".

5 CIM Source Administration

Overview

Purpose

This chapter tells how to administer the Network Trouble Patterning software host interface to all CIM sources EXCEPT custom-configured by the NTP support organization.

Contents

Introduction

CIM Source Administration

Purpose

This chapter tells how to administer the NTP host interface to all CIM sources EXCEPT those custom-configured by the NTP support organization (procedures for these conversions are similar).

- When you add a source to NTP, you must update the reference databases to define the source and establish a software link to it.
- For sources that send file-based CDR CIMs, you must add a user ID (login) on the NTP host with a directory dedicated to receive the files:
  - CCF
  - Geoprobe
  - Sonus
  - IPDR
  - Softswitch
  - AXE TRADO
  - Alcatel MT20
  - Autoplex AMA
- NTP reference data you update and procedures you use for administration differ by source type, and other specialized procedures may be required for the source link.

When to use

When NTP is installed, the NTP support organization helps you administer the sources and RE's in your network. Afterwards you may need to add new RE's and their sources unassisted, or modify the source definition.

- Many sources send NTP CIMs from multiple RE's. Unless your network adds a new source, you may never add a source, though you add RE's.
- For direct interfaces to RE's, you typically must define a unique source EACH TIME you add a new RE. Procedures here make clear when this is necessary, as does "Description" (p. 5-12).
- You may be able to use an existing source as an example when you administer a new source.

Coordination with other administrators

NTP source administration may require you to coordinate with the administrator of the source and the administrators of REs that use the source to send data to NTP. This chapter covers only what you do on the NTP host.

Task Overview

Description

Your NTP support organization will administer the sources in your network when your system is initially installed. However, if your network adds a source, you must add it to NTP and verify the link. This table lists the various tasks and procedures for sources on the NTP system.

Task	Description	Procedures
Add a source	Select the appropriate procedure for the type of source to be added. In many cases, a source must be added only once and can collect data from many RE's. Exceptions include Succession SN05 and SN06 interfaces.	• "Add or Modify a CP source" (p. 5-28) and "Set CP-NTP link variables" (p. 5-26) • "Add or Modify a 8925 Integrated Service Assurance " (p. 5-32) • "Add or Modify an SDM Source" (p. 5-35) • "Add a Source for a Configurable Conversion" (p. 5-42)
Activate and deactivate a source	Once the source has been added, you can turn the CIM flow on or off. You can also modify the interface parameters, for example if a sources's name or address changes or you want to balance I/O processes on the NTP host.	"Activate or Deactivate a Source Link" (p. 5-17)
Monitor source links	As a part of adding all sources, you verify that the addition was successful. Afterwards, you routinely monitor the integrity of the NTP-source links.	Select the appropriate procedure from "Methods for link monitoring" (p. 5-51)
Set thresholds for silent link failures	As part of adding switches, you *dbedit* the rearch table to set thresholds that determine when link alerts indicate a NTP-source link is down or degraded. You can modify these thresholds at any time.	"Set thresholds for silent link failures" (p. 5-53)

Task	Description	Procedures
Remove sources	You will seldom use this procedure — only if a source is physically removed from your network.	“Remove a Source” (p. 5-49)

Background for Source Administration

Sources, REs, and conversions

The ultimate source for CIMs is reporting entities RE's. What NTP calls a "source" is really an element that collects or forwards data from REs to NTP. Once an entity is linked to a source, and the source is linked to NTP, that entity can appear as an RE in NTP. An entity can only report to NTP if it is linked to a source. Otherwise, it can be a distant or related entity only.

Part of adding an RE to NTP is telling NTP which source the RE will use. The source must be added to NTP before you can assign an RE to it. To assign an RE to a source you enter the name of the source in the source field of rearch table record for the RE.

For REs requiring specialized message parsers (converters), you define the converter with the value in the conv field of the rearch table together with the value in the type field of the source table.

What can be a source?

Most sources exist separately from REs, but in some cases a source can be a module on an RE, or even merely the definition in NTP of a direct interface to an RE. Broadly speaking, sources include the following types.

Type	Description	Examples
mediation system	Can forward CIMs from multiple RE's. The mediation system may modify CIM record format before forwarding the CIM to NTP	GeoProbe
EMS	(Element management system). These sources have a primary function of management of a network element or multiple elements, but they can forward CIMs from multiple RE's to NTP	CP, ISA, TMOS, TONICS
direct interface	Typically a separate source must be defined for EACH interface to an RE because the RE's network ID (CLLI) cannot be determined unless it is associated with a unique source.	Custom-configured, TOPS module on DMS switch

Source types

Sources are distinguished by whether they send CIMS in a:

- Data stream
- File-based format

Data stream sources

CIMs arriving at NTP in a data stream require specialized CIM-to-CFIM converters (message parsers). NTP provides converters for CIMS from a variety of RE's.

The specific conversion type must be specified in the conv field of the rearch table when you add an RE using a specialized converter to NTP.

File-based sources for configurable conversions

Most file-based CIMs are handled through the standard NTP configurable converter interface. Typically, files are transferred via ftp over TCP/IP and require a dedicated storage directory defined as part of adding the source to NTP.

The configurable converter interface requires CIMs in one of four standard file formats:

- Delimited ASCII - AXE TRADO, Sonus, Lucent Softswitch, Plexus (not file-based), Alcatel MT20, Autoplex PCMD (Per-Call Measurement Data)
- ASCII name-value pair
- XML - IPDR
- Binary - Geoprobe
- Binary AMA - Autoplex Release 19

Source table required for all sources

A source must be named and its type defined in the source table before you can assign an RE to it or modify other tables required to administer the source. Please note that:

- You must give each source a unique name in NTP. To verify that the name you plan to use is not already assigned to another source, use the following command to search for it in the source table: **`sui find so=source | grep source`**
- For almost all configurable conversion sources, the value in the type field of the source table is **`file`** . The exception is Plexus and PCMD, for which the value should be **`ems`** .

  Important! For PCMD also a file-based interface is supported, in addition to a socket-based interface for which the **`ems`** setting applies.
- You must define in the **`Model`** column which data table the source uses.

Example: This example shows an ems-type source named afm51 and a configurable conversion source named trado1.

```
Name      Type Tz       Model      Bdrhost       Active Cimstrg

afm51     ems  est5edt  cfim       hpn42         y      y

trado1    file est5edt  dfim       -             y      n
```

For a list of supported source types, conversions they are used for, and appropriate values for the type field, use the describe command to view information for the source Table.

Other tables for source administration

CIM I/O tables

For streaming interfaces, you must define the source interface in the appropriate CIM I/O table, such as intcpdial for TCP/IP links. See "I/O Tables for Data Stream Interfaces" (p. 5-15) for more information

Configurable converter

Sources for configurable conversions require use of the following tables to describe the source interface beyond the simple definition in the source table:

- ccconfig table
- fileconfig table

Socket-based configurable conversion sources, such as Plexus, use the:

- ccconfig table
- the appropriate CIM I/O table (such as intcpdial) to define the source interface

Source Types and REs

Which source to use for an RE?

To determine which source to use for an RE, see the summary below. You can also:

- Determine what source a similar RE uses. Capacity allowing, you may be able to use the existing source for the new RE.
- Consult with your NTP support organization and local network configuration experts.

Summary

Sources include the following (see also "Background for Source Administration" (p. 5-7)).

Source Type	Type	Source	Collects data from these RE's
file	File based	Mediation Device	Sonus and Lucent Softswitch, Autoplex AMA, Alcatel MT20, Alcatel 5020, AXE CDR
file	File based	GeoProbe	SS7 links
file	File based	TMOS (and others)	AXE 10 TRADO — can also use direct interface
file	File based	Narus (and others)	Gateways, probes, and other IP elements — IPDR
file	File based	Any other source used with the configurable converter	Other sources not specifically discussed here can send CIMs if the data is formatted for the standard configurable conversion interface. Your NTP support organization may custom-configure such an interface.
cp	Data stream	CP (communications processor)	4ESS switches
ems	Data stream	8925 Integrated Service Assurance and Network Fault Management software (see "Other terms for a ISA source" (p. 5-30))	Many switch types (typically traditional circuit switches), including: 1A ESS, 5ESS, AUTOPLEX MSC, DMS, DMS MTX, EWSD, S1240, GTD-5, and OTR TOPS on DMS or OSPS on 5ESS switch modules (OTR can also use a direct interface)
univ	Data stream	OMP (Operations and Maintenance Platform)	Lucent wireless equipment (generating messages such as CP Fail, PCMD (Per-Call Measurement Data), EvDO PCMD, and EvDO CP Fail, SDHLR OM)

Source Type	Type	Source	Collects data from these RE's
univ	Data stream	SDM (Nortel Succession Supernode Data Manager)	DMS, MTX, GSM, and Succession SN05 and SN06
ems	Data stream	Plexus EMS	Plexus CDRs
univ	Data stream	MI-Agent	NGSS (SIP Log Messages)

Tables for Source Administration

Description

The following NTP reference database tables are required to administer new sources and changes source definitions. You *dbedit* these tables.

Legend

- *1* — A source can handle multiple REs; modify the table to add the source before adding the FIRST RE the source will collect data from.
- *2* — EACH RE requires a separate source definition; modify the table to add a source for EACH RE.

  Important! For the ccconfig, intcpdial and outtcpdial tables, only ONE table is used for a source interface.

  - intcpdial or outtcpdial (TCP/IP)
  - collectors with bildtscoll (configurable converter interfaces).
- Typical usage is shown here, but in some cases, the interface may be either incoming or outgoing

For values in fields in these tables, see Appendix A, "Reference Database Tables". Also see procedures for your source type in this chapter.

Table	1AESS	4ESS	5ESS	AUTOPLEX MSC	DMS MTX MSC	DMS GSM MSC	OTR (direct) 5ESS OSPS, DMS TOPS	OTR (ISA) 5ESS OSPS,DMS TOPS	DMS	EWSD	Alcatel S1240	Alcatel 5020	Succession SNO5 and SN06	GeoProbe	AXE 10 TRADO	Lucent Softswitch	IPDRs	GTD-5	Sonus	Plexus	PCMD	Autoplex AMA, AXE CDR	Alcatel MT20	CCF Charging Collection Function	SIP Log	IMS Charging Record Support
fileconfig	-	-	-	-	-	-	-	-	-	-	-	*1*	-	*1*	*1*	*1*	*1*	-	*1*	-	*2*	*1*	*2*	*1*	-	2
ccconfig	-	-	-	-	-	-	-	-	-	-	-	*1*	-	*1*	*1*	*1*	*1*	-	*1*	*1*	*2*	*1*	*2*	*1*	*2*	2
intcpdial	-	*1*	-	-	-		*2*	*1*	-	-	-	-	*2*	-	-	-	-	-	-	-	-	-	-	-	-	-
outtcpdial	*1*	-	*1*	*1*	-	*1*	-	-	*1*	*1*	*1*	-	*2*	*1*	-	-	-	*1*	-	*1*	*2*	-	-	-	*2*	-
source	*1*	*1*	*1*	*1*	*1*	*1*	*2*	*1*	*1*	*1*	*1*	*1*	*2*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*2*	*1*	*2*	*1*	*2*	2
source_procs	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	*2*	-

Table	1AESS	4ESS	5ESS	AUTOPLEX MSC	DMS MTX MSC	DMS GSM MSC	OTR (direct) 5ESS OSPS, DMS TOPS	OTR (ISA) 5ESS OSPS,DMS TOPS	DMS	EWSD	Alcatel S1240	Alcatel 5020	Succession SNO5 and SN06	GeoProbe	AXE 10 TRADO	Lucent Softswitch	IPDRs	GTD-5	Sonus	Plexus	PCMD	Autoplex AMA, AXE CDR	Alcatel MT20	CCF Charging Collection Function	SIP Log	IMS Charging Record Support
univconfig	-	-	-	*1*	-	*1*	-	-	-	-	-	-	*2*	*1*	-	-	-	-	-	-	*2*	-	-	-	*2*	-
Related table, rearch – conv field for each RE must specify appropriate conversion for source type																										
rearch	*1*	*1*	*1*	*1*	*1*	*1*	*2*	*1*	*1*	*1*	*1*	-	*2*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*2*	*1*	*2*	-	-	2

Host TCP/IP Administration

Purpose

For NTP interfaces to sources over TCP/IP, there must be a standard entry for the source in the NTP */etc/hosts* file.

Important! For data stream interfaces only, where NTP listens for data (administered in the "intcpdial Table" (p. A-82)), the */etc/services* file on the host must have an entry corresponding to the source type as defined for the appropriate TCP_PORT_*X* variable.

Procedure

Use this procedure to administer the NTP */etc/hosts* file for a new source interface.

1 From the source administrator or your network administrator, get the machine name and IP address of the source.

2 Log on the NTP host as **`root`** .

3 Use a text editor (such as *vi*) to add to the NTP /etc/hosts file an entry that includes the source's TCP/IP address and machine name, separated by a tab character.

Example:

```
555.5.55.55             abcsim
```

See your NTP host reference documentation for information on administering the /etc/hosts file.

4 If you are adding a data stream interface, note the machine name, as you will need it to dbedit the intcpdial or outtcpdial table.

END OF STEPS

I/O Tables for Data Stream Interfaces

Description

You define the source links for data stream interfaces by using the dbedit command on the appropriate CIM I/O table. You use these tables when you:

- Add a source to NTP or change its name,
- Change the source's name or TCP/IP address
- Want to balance I/O processes to the host.

To tell NTP to...	Put a source in this CIM I/O table
LISTEN for the source to send data over TCP/IP	"intcpdial Table" (p. A-82)
REQUEST the source to send data over TCP/IP	"outtcpdial Table" (p. A-119)

Typically, you first add a source but leave the source links in an inactive state until administration is done for the REs that will use the source. See Step 3 in "Activate or Deactivate a Source Link" (p. 5-17).

Which I/O table to use?

Consult with the source administrator and your NTP support organization to select the appropriate connection method for a given source. This table lists typical usage. Other configurations may be possible for a given source.

Important!

- Consult with your NTP support organization to have the 8925 Integrated Service Assurance (ISA) administrator build the pattern file for capturing EWSD CIMs (see Appendix D, "Set Up 8925 Integrated Service Assurance").
- To use ISA as a source for Succession SN05/SN06 or DMS MSC switches, consult with your NTP support organization and the ISA administrator to build the pattern file for capturing Succession SN05/SN06 or DMS MSC CIMs (see Appendix D, "Set Up 8925 Integrated Service Assurance").

This source...	For this Retype...	Typically uses...
CP	4ESS	intcpdial
ISA	1A ESS, 5ESS (not using the TCP feature), DMS, EWSD, S1240 or AUTOPLEX MSC	intcpdial (although ISA TIPS feature (if used) enables use of outtcpdial.)
	5ESS (using the TCP feature)	outtcpdial (sometimes intcpdial, not both)

This source...	For this Retype...	Typically uses...
SDM	Succession SN05 and SN06, or DMS using an SDM as a source. One source per RE.	intcpdial (sometimes outtcpdial, not both)
Plexus EMS	Plexus	outtcpdial
Autoplex OMP	PCMD	outtcpdial
MI-Agent	NGSS	outtcpdial (configured to connect to a local port)

Activate or Deactivate a Source Link

Purpose

Once a source has been added to NTP, you can turn CIM flow on or off for that source. Doing this affects data for all RE's that use the source.

For how to initially assign an RE to a source, see Chapter 4, “Add Network Elements” .

Activation Procedure

The source table contains an active field that determines whether a source is active or not. Valid values are **`y/n`** . This value can be toggled with dbedit.

Subdirectories for configurable conversion sources

The first time you activate a newly-added source for a configurable converter, three empty subdirectories are created in the directory you made in the procedure to add the source.

- error - errored records that can be reprocessed after correcting the errored record The administrator should clean up this directory.
- processed - files that have been processed recently. This directory is cleaned up periodically by cron.
- garbage - files that couldn't be processed. Possible reasons might be that the file couldn't be opened or had a bad file name. This directory is cleaned up automatically.

See “Assign or Modify FDC Group and Network Group/Segments for BB-GUI Users” (p. 7-28) for information on the role of these directories in procedures you perform to reprocess CDRs.

Task overview

To turn CIM flow from a source on or off you can use **`dbedit`** for all sources. See “Activate or Deactivate a Source Link” (p. 5-17) .

Procedure

Use this procedure to start or stop CIM flow from a source, for ALL RE's that use the source.

Before you begin

You must know the name of the source, from the name field in the “source Table” (p. A-149) and the table used to define the source interface (see “Activation Procedure” (p. 5-17)).

For steps using **dbedit** , see "Dbedit" (p. 3-17) . For field values in database tables, see Appendix A, "Reference Database Tables" . For how to use the *vi* editor, see "Edit (vi) ASCII Files" (p. 3-13) .

1 Use **sui find** to copy into a temporary file (temp) the record for the source you want to modify from the source table.

Example: To copy the collectors record for the source named nj01sm (note that the key field is Source, enter):

```
sui find source=source search=name=nj01sm noheader delim='";
"' > temp
```

```
Name      Type Tz       Model    Bdrhost      Active Cimstrg
nj01sm    univ est5edt cfim     hpn42        y      y
```

2 Edit the temp file with a text editor (such as *vi*), and save the file.

- To stop data flow from the source, change y to *n* in the Active field.
- To start data flow from the source, change n to *y* in the Active field.

3 Use **dbedit** with the **-u** (update) option to move the change from the temp file to the table you want to modify.

Example: To modify the collectors table, enter

```
dbedit -u -t source -f temp -s";"
```

4 Use **sui find** to check your changes.

Example: To check the change to the bdat1 source enter

```
sui find source=source search=name=nj01sm noheader delim='";"'
```

END OF STEPS

Configuring Incoming TCP Ports (intcpdial)

Purpose

For TCP/IP links defined in the intcpdial table, the system automatically detects which ports it needs to monitor for incoming connections. (For users familiar with the TCP_PORT_*X* variables, these are no longer used to configure incoming TCP Port connections.) This means that there is no longer a limited number of incoming TCP ports that can be used to service connection requests.

All incoming TCP sources must be configured with at least one incoming port, and a secondary host and port may be defined for redundancy. These port numbers:

- Are used in the Origin1 and Origin2 fields of the NTP "intcpdial Table" (p. A-82) for a specific source.
- Must be assigned in the /etc/services file on the NTP host.

  Important! A given host and port may only be used for a single source. Once a host and port are defined, they cannot be used again for any other source.

Procedure

Important! You will seldom use this procedure. When your NTP support organization installs your NTP system, they normally set up the etc/services file for the various types of sources.

Use this procedure to edit the /etc/services file and add appropriate port information.

1 Log on the NTP host as **`root`**.

2 Use a text editor (such as *vi*) to open the */etc/services* file.

- Find a port number that is unassigned that you can use for the TCP/IP connection this type of source.
- Edit the file to assign the port.
- Note the port number you assigned. You will need it later when you administer the "intcpdial Table" (p. A-82).

See the reference documentation for your operating system for information on the */etc/services* file.

END OF STEPS

Add a directory for a file-based source

Purpose

Each source that sends file-based CIMs to NTP — usually CDR CIMs — must have its own login ID and directory on the NTP host. You create these by using standard operating system procedures for your platform.

Procedure

Use these guidelines to create a login and directory for a file-based source.

1 Use standard administrative procedures for your operating system to add a user ID (login) and directory on the NTP host. Follow the guidelines.

- An entry should be created in the /etc/passwd file, and the ID (UID) should be unique.
- Assign the *sh* shell to the login.
- Assign the directory the permissions *7-5-5* (full permissions for self and read-execute for self and other).
- If you already have a source of the same type in your network, we recommend you assign the same user group as the existing source. To determine this, do the following:
  - Use **`sui find so=fileconfig noheader delim='";"'`** to find the source in the bildtscoll table. This sample output shows a source of collector_name bdat1 and conversion_name bill-ericsson.

    ```
    #Collector_name;Conversion_name;Dir_list;Io_name
    bdat1;bill-ericsson;/susr/bdat1/;bdat1
    ```
  - Look at the source_names entry in the */etc/passwd* file, and note the number for its user group. In the example above for bdat1 the entry the user group is 20 (fourth field). The same value appears in the */etc/group* file for bdat1.

    ```
    bdat1:*:106:20:UNIV User#1:/susr/bdat11:/usr/bin/sh
    ```

2 Give the login (and password) to the source administrator and ask him or her to set up the same login as a user on the source.

3 Note the following items, as you will need them to add the source to NTP in "Add a Source for a Configurable Conversion" (p. 5-42):

- The login you created, which you will use it in the:
  - Name field of the source table
  - Source field of ccconfig and fileconfig
- The directory you created (for example /home/bdat1), which you will use in the Dir_list field in the fileconfig table

END OF STEPS

Create Working Versions of Converter Files in $USERDIR

Purpose

All product provided converter files, such as fetcher configurations (**.cfg** files), filters, and fetchers, are delivered in the **$MODELDIR** directory. The product can change these files in every release, and an upgrade is not expected to save or preserve those changes.

Customers specific changes reside in **$USERDIR**.

If 8920 NTP does not find the customized converter files in **$USERDIR**, it will use the files supplied with the product from **$MODELDIR**.

Procedure

Use the following procedure to create working versions of converter files in **$USERDIR**:

1 Create a directory **$USERDIR/fetchers_cfg**

2 Copy the **$MODELDIR/** <*type of files*> **_fetcher.cfg** template file to **$USERDIR/fetchers_cfg**

3 Use a text editor (such as **vi**) to change the file, as needed.

Additional information When populating the **fileconfig** reference table, add the following line to the **filefetcher** field:

-f $USERDIR/fetchers_cfg/ <*type of collector*> **_fetcher.cfg**

The complete contents of the **filefetcher** field should resemble this:

<*type of collector*> **_fetcher -f $USERDIR/fetchers_cfg/** <*type of collector*> **_fetcher.cfg -e $MODELDIR/** <*type of collector*> **_filter**

END OF STEPS

Filter files

Use the same procedure for <*type of collector*> **_filter** files. Note that the complete contents of the **filefetcher** field should resemble this:

<*type of collector*> **_fetcher -f $USERDIR/fetchers_cfg/** <*type of collector*> **_fetcher.cfg -e $USERDIR/filters/** <*type of collector*> **_filter**

CP Sources

Overview of CP Sources

Purpose

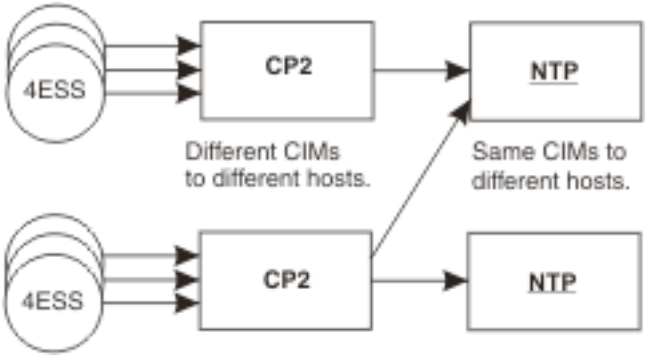
This section explains administration you do on the NTP host for a CP source.

For CP administration you do on CPs and for detailed information on CP configurations, see *CP Administration and O&M*.

CP configurations

CPs collect data from 4ESS switches and forward it to NTP. A switch can send data to only one CP, but a CP can integrate with many switches, and NTP can integrate with multiple CPs. A configuration may have multiple NTPs.

- *Multiple switches.* Up to 75 4ESS switches can be linked to one CP. (A switch can send its data to only one CP.)
- *Multiple CPs.* If you have more than 75 4ESS switches reporting to NTP, you must have at least two CPs.
- *Multiple hosts.* A CP can send data to as many as four NTP hosts. Typically, each host receives the same data. For example, you could have NTP running on one CP in New York (NTP 1), and another in Albany (NTP 2) and users could log on either.

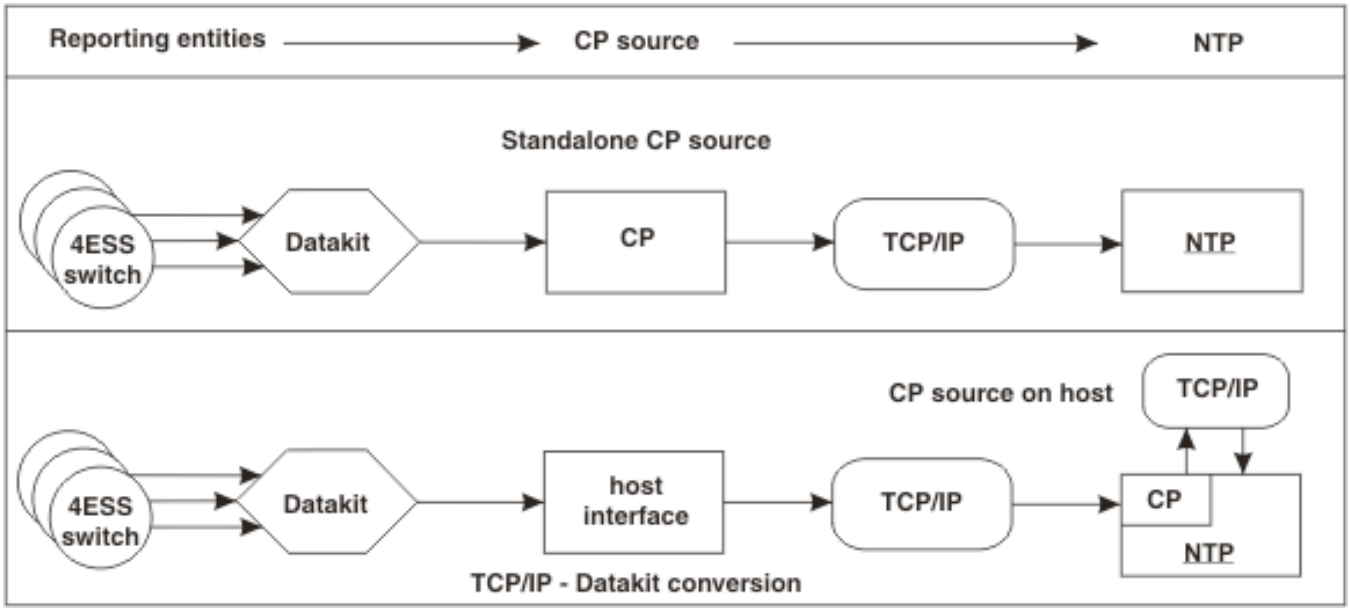


The CP can run either on its own machine (standalone) or on the NTP host. The CP and the NTP host communicate over TCP/IP. A Datakit-TCP/IP interface is required between the RE's and a CP on host since the host platform does not support Datakit connections. For standalone CPs, communication between the switches and the CP is over Datakit links. Two-way communication is supported, but data flow is from the switch to NTP. The CP calls the NTP machine to initiate a connection over one of its TCP/IP ports.

Illustration of CP data flow

This illustration summarizes the basic configurations, the links, and the data flow for CPs.For administrative purposes, you can usually proceed as if a CP on host is really a standalone CP. Illustrations and procedures in the rest of this section are for standalone CPs, but they also apply to CPs on host.

Important! For multiple links, use relevant procedures multiple times.



Coordination

This table shows who to coordinate with for administering CP links for 4ESS switches.

This person	Does this...	Reference
CP administrator	Adds, deletes, modifies. and monitors 4ESS-CP and CP-host links, from the CP viewpoint.	CP Administration and O&M
TCP/IP-Datakit interface administrator	Administers the customer-installed TCP/IP-Datakit interface required between the switch and the CP for some configurations.	Appendix D in the NTP CP Administration and O&M book.
Datakit administrator	Provides Datakit dialstrings for 4ESS switches, CPs, and the host.	Datakit manuals
4ESS administrator	Installs or removes 4ESS switches.	4ESS manuals
NTP support organization	Initially installs the CP or CPs. Solves CP and NTP problems not covered in manuals.	None

Add or Modify a CP Source

Overview

Rarely, you may need to modify the CP-NTP link variables set on the NTP host. You may do this when the first CP is added to NTP, or as necessary. System variables control how NTP determines the status of a CP-NTP link and reports it in link alert messages. These variable are set when NTP is installed. See “Set CP-NTP link variables” (p. 5-26).

Otherwise, the following procedures contain all the necessary administrative steps to add a CP.

Set CP-NTP link variables

Purpose

You use the **`sui setsys`** command to view or modify the CP-NTP variables that define link alerts. The following table describes the CP-NTP variables.

Consult with your NTP support organization before modifying these variables.

Important! The link status message also has a field reporting the status of the switch-CP Datakit link. This status indicator is not a variable.

Variable	Description
ZM (zero message interval)	ZM determines the 4ESS-CP link status and specifies how many ZM intervals can occur before NTP generates a link alert message. Each CP records the number of messages received on each link in its link status message. When NTP receives a link status message reporting zero messages received, it counts the 5-minute interval since the last link status message as a zero message interval for that switch-CP link. • *Down*. When the count of zero message intervals exceeds the value of ZM, the switch-CP link is "down" and NTP generates a link alert message. For ZM of 3, the switch-CP link is down if the CP reports no messages received from the RE for the last three intervals (15 minutes). Default value: 2 (two link status messages report no messages received from the same switch in 10 minutes). Range: 0 to 120. When ZM is 0, the switch-CP link status is not determined by the number of messages received.
UM(1, UM2 (percent unreadable messages)	UM1 and UM2 determine the 4ESS-CP status. NTP divides the value of the Number of Messages Unreadable field in the link status message by the value of the Number of Messages Received field in the link status message to derive a percentage. • *Down (UM1)*. The link is "down" if the percentage of unreadable messages equals or exceeds the UM1 threshold. Default: 70 (70% of link status messages unreadable). Range: any integer value greater than UM2 and no greater than 100. • *Degraded (UM2)*. The link is "degraded" if the percentage of unreadable messages equals or exceeds the UM2 threshold. Default: 30 (30% of link status messages unreadable). Range: any value greater than 0 and less than the value of UM1. • *Up*. The Switch-CP link status is "up" if the percentage of unreadable messages is less than UM2, the number of zero messages is less than ZM, and the number of link failures is less than LF2.

Variable	Description
LF(1, LF2 (number of link failures	LF1 and LF2 control the link status information used in generating link alert messages by determining how many times the CP detects switch-CP link failures in each 5-minute interval. • *Down.* The switch-CP link is "down" if the number of link failures detected equals or exceeds the threshold set for LF1. Default: 2 (two link failures detected). Range: any integer value greater than the value of LF2 (the default is 1) and no greater than 255. • *Degraded.* The switch-CP link is "degraded" if the number of link failures detected equals or exceeds the threshold set for LF2. Default: 1 (one link failure detected). Range: any integer value greater than zero and less than the value assigned to LF1. • *Up.* If the number of link failures is less than LF2, the number of zero messages is less than ZM, and the percentage of unreadable messages is lower than UM2, the link is "up." If either LF1 or LF2 exceeds 3, the switch-CP link status is not determined by the number of link failures.

Add or Modify a CP source

When to use

You do NOT need to do this each time a you add an RE. Many RE's can be integrated through a single CP.

Purpose

Before you begin, please note that:

- Administration is also required on the CP. For what to do on the CP, see CP Administration and O&M.
- You do not need to do this each time you add an RE. Once the CP is added, you can administer many RE's to send data to NTP through it.

Procedure

Use this procedure to add a CP source to NTP.

For steps requiring **`dbedit`**, see "Dbedit" (p. 3-17). For information on values for fields in database tables, see Appendix A, "Reference Database Tables".

1 Add an entry for the CP in the NTP /etc/hosts file.

Hint: See "Host TCP/IP Administration" (p. 5-14).

2 Log on NTP as **`ntp`**.

3 If you have not already done so, dbedit the rearch table, adding or modifying records for each 4ESS switch that sends its CIMs to the CP.

Important! The tag in the rearch table must match the link number defined on the CP, (which is the link number in the CP's LINK database table). See "rearch Table" (p. A-129), and Chapter 3, "4ESS-CP Links" (LINK database table in CP Administration and O&M.

4 **`dbedit`** the source table to add a record for the new CP. This names the CP as a new source.

Set the Active field to n until later in this procedure.

Hint: See "source Table" (p. A-149) *and* "Host TCP/IP Administration" (p. 5-14) *for details*.

5 **dbedit** the "intcpdial Table" (p. A-82) to add a record defining the TCP/IP port number the CP uses to call NTP.

- The machine name in the Origin1 field must match the entry for the source in the /etc/hosts file (see Step 1).
- The port number in the Origin1 field can be any port number. (See "Configuring Incoming TCP Ports (intcpdial)" (p. 5-19).)

  Important! You can also configure a backup (secondary) connection by entering another machine name and port number in the Origin2 field (**cpnorth1:3333** in the example). You would do this if the CP has multiple Ethernet LAN cards configured on different networks. The secondary machine must be defined in the NTP */etc/hosts* file, and the port number must be the same one used for the primary link (Origin1 field). See Chapter 4, "CP-NTP Links," in CP Administration and O&M for more information.

6 Set CP-host link variables. (See "Set CP-NTP link variables" (p. 5-26).)

7 **dbedit** the source table again, this time to change the CP's Active field to **y**.

8 Use one of the link monitoring methods to verify CIMs are moving from switches through the CP to NTP. (See "Monitor Links" (p. 5-51).)

9 Tune the link, if needed. (See "Administer Silent Link Failure Detection" (p. 5-53).)

10 Modify the CP-NTP link variable settings, if necessary. (See "Set CP-NTP link variables" (p. 5-26) for the procedure.)

END OF STEPS

8925 Integrated Service Assurance Sources

Overview

Purpose

This section explains administration you do on the NTP host for 8925 Integrated Service Assurance (ISA) and Network Fault Management software sources (Formerly Network Fault Management [NFM]).

ISA administrators install pattern files on ISA machines to define which CIMs to send to NTP. For how this and other ISA administration is done, see Appendix D, “Set Up 8925 Integrated Service Assurance”.

Other terms for a ISA source

In references, messages, or file or directory names, ISA may be referred to by the following terms:

- NFM (Network Fault Management) — The former name for ISA.
- TNM (Total Network Management) — Another former name for ISA.
- NOC1 — A scaled-down version of ISA.
- TSM (TNM Surveillance Module) — The TNM module that collects CIMs from switches.
- SCCS (Switching Control Center System) — What TNM evolved from.

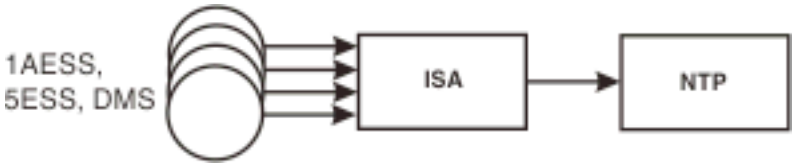
Switch types

ISAs can collect data from many of the switch types NTP supports (see “Source Types and REs” (p. 5-10)). Each ISA can only collect from one switch TYPE, however, as defined by its conversion type. (This is true of all sources of type "ems", as defined in the source table.

Illustration of ISA data flow

This illustration shows the simplest configuration for ISA sources. Links can be multiple (see the illustration in “Overview of CP Sources” (p. 5-23)).

Important! For multiple links, use relevant procedures multiple times.



Contents

Add or Modify a 8925 Integrated Service Assurance

When to use

You do NOT need to do this each time a you add an RE. Many RE's can be integrated through a single 8925 Integrated Service Assurance (ISA).

Before you begin

Before you can add a ISA on NTP, the ISA administrator must administer the ISA machine.

- *Pattern files.* A ISA- NTP distribution pattern file must be installed on the ISA machine to define which DIMs to send to NTP.
- *Interface.* The TCP/IP interface must be configured on ISA. NTP will be originating calls over TCP/IP to establish a virtual connection over fiber or ethernet to communicate with the ISA machine.

See Appendix D, "Set Up 8925 Integrated Service Assurance" for information on NTP pattern files for ISA and other ISA administration.

Procedure

Use this procedure to add a ISA source to NTP (along with procedures in Appendix D, "Set Up 8925 Integrated Service Assurance").

1 Log on the NTP host as **`ntp`** .

2 If you have not already done so, **`dbedit`** the rearch table, adding or modifying records for each switch that sends its CIMs to the ISA.

3 **`dbedit`** the source table to add a record for the new ISA. This names the ISA as a new source.

Set the cimstrg field to:

- **`y`** - allow raw CIMs to be stored in the database (traditional NTP functionality)
- **`n`** - do not store CIMs (used to conserve database space)

Important! CIM is set on a per source basis. All offices connected to a source are affected.

Example: For a new ISA to be named nfm1, add this record. If you do not have the optional RDS feature (6214, refsynch), put a dash (-) in the Bdrhost field.

```
Name            Type Tz          Bdrhost        Active  Cimstrg

nfm51           ems  est5edt     hpn42          y       y
```

See "source Table" (p. A-149) for information about the source table.

4 Determine the appropriate interface method and NTP reference table (see "I/O Tables for Data Stream Interfaces" (p. 5-15)) to use for this source.

5 Are you using a TCP/IP interface (intcpdial or outtcpdial)?

- If NO, go to the next step.
- If YES, use the procedure in "Host TCP/IP Administration" (p. 5-14) to add an entry for the ISA source in the /etc/hosts file.

6 **`dbedit`** the appropriate I/O table to add a record for this ISA that defines the TCP/IP address that NTP software uses to interface with this ISA unit.

In the Source table, set the Active field to:

- **y** - if the other-end sources is set up and you are ready to collect data
- **n** - if you are not ready to collect data. If you set this field to n, you must change the active field to y when you are ready.

Use one of the link monitoring methods to verify CIMs are moving from switches through the ISA to the NTP. (See "Monitor Links" (p. 5-51) .)

7 Tune the link, if needed.

8 Edit the rearch table, adding or modifying records for each switch that sends its CIMs to the ISA.

END OF STEPS

SDM Sources

Overview of SDM Sources

Background

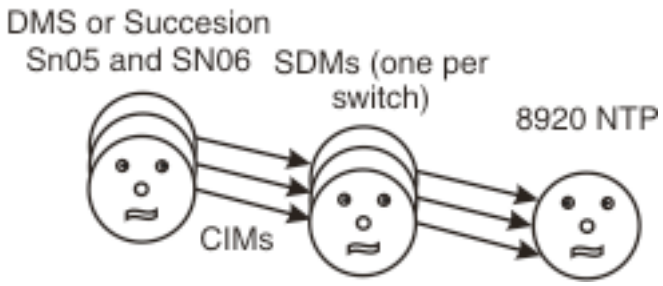
In the past, NTP collected CIMs from DMS switches only through 8925 Integrated Service Assurance (ISA) sources.

Now, NTP can receive CIMS from a DMS or Succession SN05 and SN06 switch directly from a supernode data manager (SDM).

For this type of interface to NTP, a separate SDM source is required for EACH DMS or Succession switch.

Illustration of SDM I/O

This illustration shows a high-level view of the direct SDM interface, with one SDM per switch.



Important! CIMs can also be routed through SDMs to a ISA source. In that case, the SDMs are invisible to NTP. You would simply add the ISA source to NTP (see “Add or Modify a 8925 Integrated Service Assurance ” (p. 5-32).

Add or Modify an SDM Source

Purpose

Use this procedure if you have a new DMS or Succession SN05 and SN06 switch and you want NTP to receive its CIMs directly from an SDM. This procedure:

- Adds an SDM to NTP as a CIM source
- Establishes CIM flow between the SDM and NTP

Administration on the SDM

The SDM can be configured as either a client that establishes a connection to NTP or server that listens on a specified port for a NTP-initiated connection. (In either case, the flow of messages is one-way from the SDM to NTP.) Setup is required on the SDM if it is to act as a server. See information on adding a log device, using Logroute, in the vendor-supplied *Fault Tolerant User Guide* , 297-5061-906. Follow the directions for connecting to a TCP-in device and specifying which port the SDM is to listen on.

Important! This procedure assumes the SDM is configured as a client (but see Step 6).

Procedure

Be sure to add a separate SDM source for EACH DMS or Succession SN05 and SN06 switch (see "Overview of SDM Sources" (p. 5-34)).

.

1 Log on NTP as **root** .

2 Add an entry for the SDM in the NTP */etc/hosts* file. (See "Host TCP/IP Administration" (p. 5-14) .)

3 Log on NTP as **ntp** .

4 If you have not already done so, **dbedit** the rearch table, adding or modifying the record for the switch that sends its CIMs to the SDM.

Important! Enter **3 M** as the value in the conv field.

5 Use **dbedit** to add the SDM to the source table.

Set the Active field to **n** until later in this procedure.

Important! Enter **univ** as the value in the type field.

6 Use **dbedit** to add new SDM to the intcpdial table (but see the note below).

Important! The machine name in the Origin1 field must match the entry for the source in the */etc/hosts* file (see Step 2).

(A link using outtcpdial is also supported. See "Administration on the SDM" (p. 5-35) .)

7 Use **dbedit** to create a record in the univconfig table for the SDM to specify the values the switch uses for start of message (som field, typically 31) and end of message (eom) field, typically -).

Important! Characters for start and end of message can be configured on the switch. Consult the switch administrator to determine the correct values. You must determine the numeric value for control characters. Values for commonly-used characters are: **31 for Control-** _ (unit separator), **25 for Control-Y** (end of medium), and **3** for **Control-C** (end of text). See your local documentation on the ASCII character set to determine the numeric value for any other control characters.

Example:

```
Source     Config    Som    Eom

sdm01      source    31     -
```

8 **dbedit** the source table again, this time to change the Active field to **y** .

9 Use a link monitoring methods to verify CIMs are moving from the switch through the SDM to NTP. (See "Monitor Links" (p. 5-51) .)

10 Tune the link, if needed. (See "Administer Silent Link Failure Detection" (p. 5-53) .)

END OF STEPS

OTR Sources

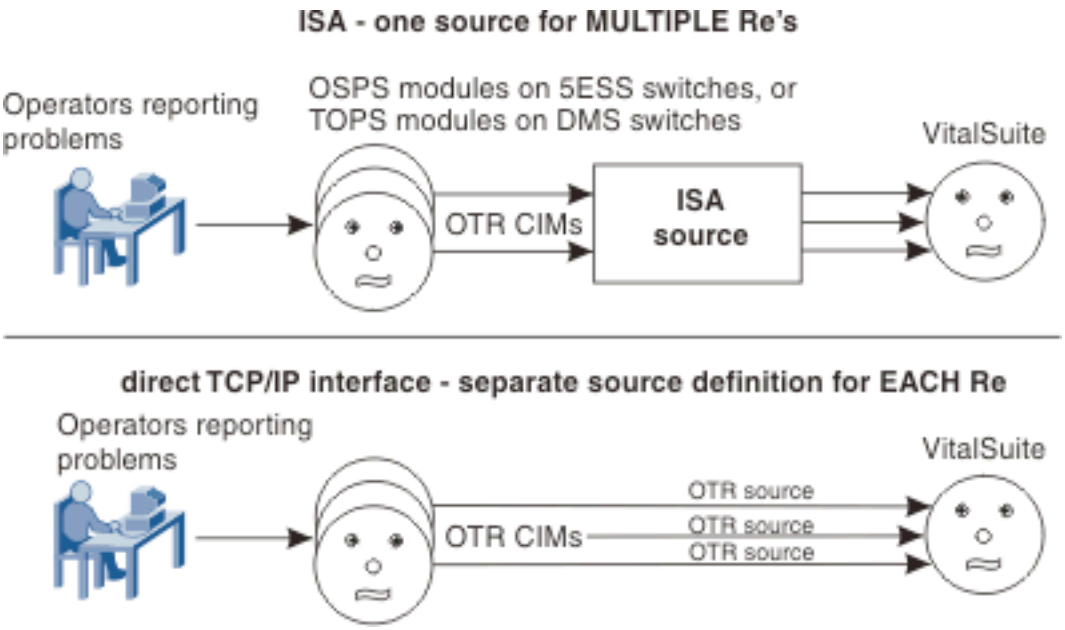
Overview of OTR Sources

Purpose

OTR RE's include OSPS modules on 5ESS switches and TOPS modules on DMS switches OTR CIMs can come to NTP either through 8925 Integrated Service Assurance (ISA) OR through a direct interface. This section explains how to define the OTR source in NTP for the two configurations.

Illustration of OTR (OSPS, TOPS) I/O

This illustration shows a high-level view of the two configurations for OTR CIM flow — through ISA or through direct interface. With ISA, multiple OTR RE's can use the same ISA source. But a direct interface, a SEPARATE source must be defined in NTP for EACH RE. This is because NTP can only derive the RE's CLLI by association with a unique source.



Background — OTR RE's

The conversion type you select in the rearch table for OTR RE's depends on what source will be used.

In the conv field of the rearch table:

- For a ISA source, use **ems**
- For a direct interface, use **osps** (for 5ESS OSPS) or **tops** (for DMS TOPS)

Add an OTR (OSPS, TOPS) source

8925 Integrated Service Assurance (ISA)

To define ISA as a source, follow the steps to add a ISA source in " 8925 Integrated Service Assurance Sources" (p. 5-30).

- Use **ems** in the type field of the source table:
- To define a direct interface as a source, add a SEPARATE and unique source for EACH OTR RE. Use the following values:
  - For OSPS, use **osps** in the type field of the source table
  - For TOPS, use **tops** in the type field of the source table.

Sources for Configurable Conversions

Overview of Sources for Configurable Conversions

Purpose

This section explains administration you do on NTP for sources that send CDR CIMS to NTP using the configurable converter interface. These include:

- IPDR
- AXE TRADO
- Softswitch
- Sonus
- Plexus
- Geoprobe
- PCMD
- MT20
- AXE CDR
- Autoplex AMA

Procedures for consultant-configured conversions are similar.

CDR (IPDR) sources

Currently, with the exception of the Plexus and PCMD source types, all configurable conversion integrations are file-based interfaces for CDRs. The source sends CDR CIMS in file format over an ftp link to a directory on the NTP host that has been created as part of adding the source. The source is typically a mediation device, though it can be a direct interface, or any element that sends files in acceptable format (see "What can be a source?" (p. 5-7)). Examples include TMOS, and Narus. To administer NTP for these sources, however, you only need to know the directory, the file format, and the conversion based on the file format.

The Plexus source type is socket-based. These sources must be added manually. See "Manually add a configurable converter source" (p. 5-43).

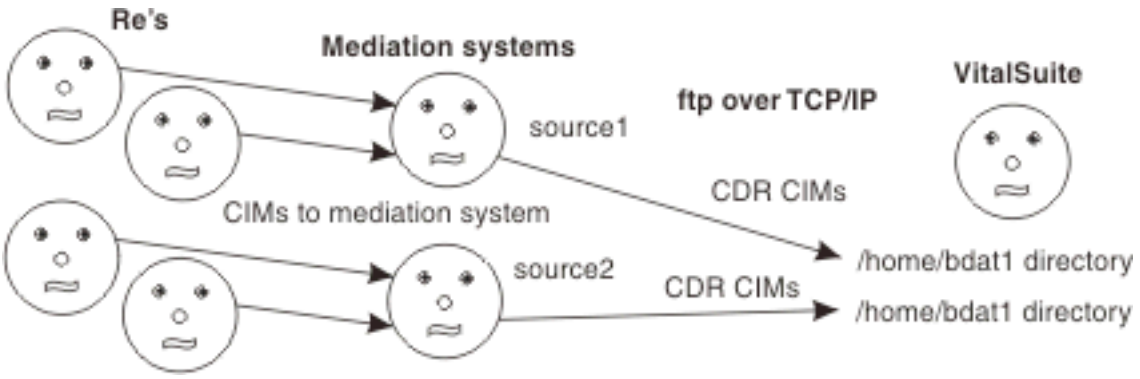
> **Important!** For PCMD also a file-based interface is supported, in addition to a socket-based interface for which the **`ems`** setting applies.

Multiple RE-spawns

If a source RE-spawns more than 10 times in a 5-minute period, the source is shut down, the active field in the source table is changed to no, and a minor error is logged in the master log.

Illustration of configurable conversion source data flow

In this illustration, NTP receives data from two mediation systems, bdat1 and bdat2. Directories on the NTP host enable bdat1 to put its CDRs in the /home/bdat1 directory and bdat2 to put its CDRs in the /home/bdat2 directory.



Add a Source for a Configurable Conversion

Purpose

To Add or Modify a Source for Configurable Conversion, see "Manually add a configurable converter source" (p. 5-43)

In these procedure you:

- Create a login on the NTP host for the source so data files transferred from the source can be stored in the source's home directory.
- Define the source in the NTP reference tables

Before you begin

Before you begin, do the following:

- Consult with the source administrator and your network administrator to determine the machine name and IP address of the source.
- Be sure to, **`dbedit`** the rearch table to define each RE that sends its data to the source (see "Add an entity to rearch" (p. 4-64)). The value in the conv field should be:
  - IPDR — *ipdr*
  - AXE TRADO — *axetrado*
  - Lucent Softswitch — *softsw*
  - Others - *custom*

Manually Add a Source for Configurable Conversion

Manually add a configurable converter source

Purpose

Use this procedure to manually add a CC source to NTP. This is most often used for the SIP Log, Plexus and TCP/IP socket based PCMD source.

References

For steps requiring *dbedit* , see “Dbedit” (p. 3-17) . For information on values for fields in database tables, see Appendix A, “Reference Database Tables” .

Important! If you are using the optional SIP Log feature, you need to make sure that the *ssh* tunnel is configured before you add a CC source. For information on configuring the ssh tunnel, see “OTR Sources” (p. 5-37) .

Procedure

1 Log on the NTP host as *ntp* .

dbedit the source table to add a record for the new source.

2 Set the cimstrg field to:

- **y** - allow raw CIMs to be stored in the database (traditional NTP functionality)
- **n** - do not store CIMs (used to conserve database space)

Important! CIM storage is set on a per source basis. All offices connected to a source are affected.

Example: For a new source to be named sfms, add this record. Ifyou do not have the optional RDS feature, put a dash (-) in theBdrhost field.

```
Name    Type Tz        Model     Bdrhost        Active Cimstrg
sfms    ems  est5edt   cfim      hpn42          y      y
```

(See “source Table” (p. A-149) for information about the source table.)

3 *dbedit* the rearch table, adding or modifying records for each switch that sends its CIMs to the source.

4 Determine the appropriate interface method and NTP reference table (see "I/O Tables for Data Stream Interfaces" (p. 5-15)) to use for this source.

5 Is this a PCMD or SIP Log source?

- If no, continue with Step 6.
- If yes, continue with this step.

Add an entry for the source in the univconfg table (see "univconfig Table" (p. A-163)), where *SOURCE* is the source name specified in the source table (see "source Table" (p. A-149)), and the other options are set as shown in the following example.

Example:

```
SOURCE          CONFIG              SOM         EOM
pcmd            pcmd                1           3
```

or

```
SOURCE          CONFIG              SOM         EOM
sip1            siplog              1           3
```

6 Are you using intcpdial or an incoming TCP/IP?

- If NO, go to the next step.
- If YES, use the procedure in "Host TCP/IP Administration" (p. 5-14) to add an entry for the source in the /etc/hosts file.

7 *dbedit* the appropriate I/O table to add a record for this 8925 Integrated Service Assurance (ISA) that defines the TCP/IP address that NTP software uses to interface with this ISA unit.

8 Populate the ccconfig table for the new source.

For Plexus, use the following values:

- source — the name used when the source table was created
- collector type — plexus

- format — delimval
- conversion_name — plexus

For Autoplex PCMD, use the following values:

- source — the name used when the source table was created
- collector type — pcmd
- format — delimval
- conversion_name — pcmd

For SIP Log, use the following values:

- source — the name used when the source table was created
- collector type — siplog
- format — freefmt
- conversion_name — siplog

9 In the Source table, set the Active field to:

- **y** — if the other-end sources is set up and you are ready to collect data
- **n** — if you are not ready to collect data. If you set this field to **n** , you must change the active field to **y** when you are ready.

For SIP Log you should not set the Source to active until completing the rest of the steps.

For explanations of the fields in these tables, see the individual table descriptions: "intcpdial Table" (p. A-82) or "outtcpdial Table" (p. A-119) .

10 Use one of the link monitoring methods to verify CIMs are moving from switches through the source to the NTP. (See "Monitor Links" (p. 5-51) .)

11 Tune the link, if needed. (See "Administer Silent Link Failure Detection" (p. 5-53) .)

12 Edit the rearch table, adding or modifying records for each switch that sends its CIMs to the ISA.

Important! If you are not using SIP Log, stop, you are done with this procedure. If you are using SIP Log, continue with Step 13.

13 For SIP Log you need to establish the *ssh* tunnel by adding an entry in the source_procs table (see "source_procs Table" (p. A-150)) containing two fields: **SOURCE** and **EXECUTABLE** .

Important! Make sure your Firewall permits both outgoing and incoming connections on the NTP and MI-Agent local ports.

Example:

```
Source
sip1

Executable
/usr/5bin/ssh -N -L 20000:localhost:9095
   username@simntp1.pl.lucent.com
```

where:

sip1 - an example of source name specified in the source table

20000 - number of a local ntp port that NTP will connect to (you populate outtcpdial with this value and it has to exceed 1024)

9095 - number of a local MI-Agent port that awaits connections

username - username on MI-Agent

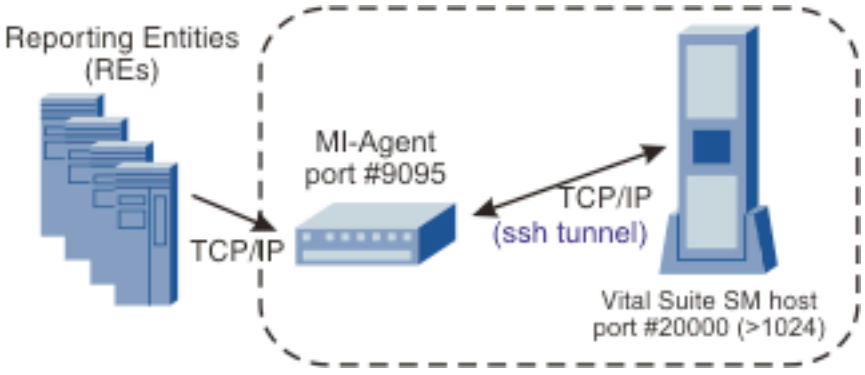
@simntp1.pl.lucent.com - an example of IP address/fully qualified domain name of MI-Agent

Mandatory *ssh* options:

-N - do not execute a remote command

-L - specifies that the given port on the local (client) host is to be forwarded to the given host and port on the remote side

The picture below shows how the *ssh* tunnel between NTP and MI-Agent is established for the SIP Log feature.



END OF STEPS

Configure the ssh tunnel

Purpose

Important! Use *ssh version 2* in order to increase the security of information transfer.

MI-Agent has to be configured properly in order to authorize the public key.

Use this procedure to configure the ssh (secure shell) tunnel. The *ssh* tunnel is used for SIP Log in order to establish the connection between NTP and MI-Agent.

1 Log on the NTP host as *ntp*. (You must be logged on as *ntp* to proceed.)

2 Enter either

- **`ssh-keygen -t rsa`** (for RSA - an algorithm for public-key encryption)

or

- **`ssh-keygen -t dsa`** (for DSA - Digital Secure Algorithm)

Result: You are prompted to enter the file in which to save the key or use a default one. Press Enter.

3 You are prompted for a password phrase (passphrase). Leave it empty by pressing Enter twice.

Result: You see the location where your public and private keys have been saved and the key fingerprint.

Your keys are now generated and located at: */lucent/ntp/snas/snas/.ssh*

id_rsa or *id_ds* - private

id_rsa.pub or *id_dsa.pub* - public

In order to initiate the first ssh connection you have to add the public key to the *authorized_keys* file on MI-Agent (which most often is located at */home/username/.ssh*).

4 Enter **`ssh -l username IP address/fqdn MI-Agent`**

Result: You are asked if you want to continue connecting.

5 Enter **`yes`**

Result: The *ssh* tunnel configuration is complete.

END OF STEPS

Remove a Source

Overview

Purpose

This section provides a high-level procedure to remove a source from NTP. Basically, you must undo the steps taken to add the source.

The source administrator may also need to remove NTP from the source.

- For 8925 Integrated Service Assurance (ISA), see Appendix D, "Set Up 8925 Integrated Service Assurance".
- For CPs, see *CP Administration and O&M*.

Contact your NTP support organization to work with the source administrator.

Procedure

Contact your NTP support organization, if necessary, to help in using this procedure to remove a source from your NTP system. For steps requiring *dbedit*, see "Dbedit" (p. 3-17).

1 For incoming sources, use a text editor (such as vi) to remove the entry from the:

- */etc/hosts* file if I/O is over if TCP/IP

2 Use *dbedit* to remove (or modify) records for the source in the rearch table (source field), and any routing database records, if they exist.

3 Use *dbedit* to remove records for the source from the other reference database tables:

- File-based sources — ccconfig and fileconfig
- Data stream-type sources — appropriate CIM I/O table, either intcpdial or outtcpdial
- Universal sources — univconfig table

4 Use **`dbedit`** to remove the source from the source table.

5 (File-based sources only) Use the appropriate procedure for your operating system to remove the login and home directory that were created for the source on the NTP host.

6 Inform the administrator of the source that NTP is no longer using the source.

END OF STEPS

Monitor Links

Overview

Purpose

Links connect REs to sources, and sources to the NTP host. This section lists the methods for monitoring those links. (See also Chapter 10, “Routine Monitoring” .)

Methods for link monitoring

Use the following methods to monitor links.

Method	Description	Reference
Use the **`sui trapcfim`** command.	Lists CFIMs as they arrive.	“Example: trapcfim output” (p. 5-52)
Use the **`sui linkmon`** command	Monitors links between RE's and sources/sources and NTP.	“Syntax for dbedit” (p. B-20)
Use the **`sui find`** command with the following options: *sui find so=linkstatus se=status=up*	Shows which links are currently up.	None
Use a text editor to view the appropriate log in $LOGDATA:	-	• “lnkpm Log” (p. 10-31) • “sccs Log” (p. 10-35) • “univlog Log” (p. 10-37)
Use the *audit.re, audit.link* , and *audit.de*	-	Consult your NTP support organization.
Have CIMs rerouted to a file where you can verify they are arriving.	Your NTP support organization typically does this when a source is first added. Otherwise, this is a last resort, since it disrupts normal CIM processing.	

Example: trapcfim output

- To see data arriving at NTP from a reporting entity, enter **`sui trapcfim se=re=re_name`** (where *`re_name`* is the value in the RE field in the rearch table, typically a CLLI code).
- To see all data arriving at NTP from a source, such as cpn1, enter **`sui trapcfim se=source=sourcename`** (where sourcename is the source as administered on NTP.).

This example shows output from the **`sui trapcfim`** command.

```
Date         Time     Cpdigits      Digits
03/10/06     11:06    7812186517    9956436726
03/10/06     11:06    6315256350    8009111358

Cust      Cpcust    Durat    Fdc Ct   St
-         -         -        qos 720  020
-         -         -        nca 031  -
```

Your interest in this output is the RE field, since, if an RE is in this field, you know that the links through which its CIMs reach NTP are up.

Contents

Administer Silent Link Failure Detection

Overview

Though a link to an RE may be up, NTP may receive little or no data because of a problem at the RE. This is called a "silent link failure". If little data arrives, NTP assumes the link between the RE and the source is degraded. If no data arrives, NTP assumes the link is down.

Thresholds set for a predefined interval for each entity type determine when a link is declared down or degraded. In both cases, NTP generates a link alert. When you check the source field of the link alert, its value will be "cims". You can also use the **`sui linkmon`** command to see which links between reporting entities and sources are degraded and down.

Important! When the count of CIMs received in an interval from an RE exceeds these thresholds, the link is declared to be up.

When to use

Consult with your NTP support organization before modifying the system defaults for detection of silent link failures.

Set thresholds for silent link failures

You can adjust the detection of silent link failures by using dbedit to change the link down threshold, the link degraded threshold, and the 5-minute interval count for each RE. These values are defined in the following fields in the rearch table record for each entity. (See “rearch Table” (p. A-129) for full information on these fields.)

- down
- degraded
- interval

  Important! For special cases where an RE sends CIMs to multiple sources at different rates, you may also need to modify the following field:

- calc

Verify link integrity

Purpose

Use the following procedure to verify the integrity of the links between a source and NTP. This procedure also does some data analysis.

1 Connect a source to NTP and allow it to send data for 24 hours.

2 Run **sui find** to collect the data that was received from that source during the 24 hour period (specify a source field in the search expression, as in the example below).

Example:

```
sui find source=cfim se=source=trado1 and
      datime=12/10 00:00 - 12:00 maxsave=100000
      save=cfims1

sui find source=cfim se=source=trado1 and
      datime=12/10 12:00 - 23:59 maxsave=100000
      save=cfims2

sui join from=cfim2 to=cfim1 maxsave=100000
```

You may have to use smaller segments of time ranges and more **find** commands, if more than 10000 cfims are being produced for source in a 12-hour range.

3 Run **compute** to determine which FDCs were collected during the 24-hour period (specify *fdc* in the row field). You should see a majority of the possible FDCs for the switch types connected to the source.

Example: **sui compute row=re,fdc file=cfims**

4 Check the incon log and master log, as well as other appropriate log(s) for the source type: lnkpm event log, SCCS log, or "garbage" files (for Geoprobe and configurable conversion sources).

Some typical errors seen in the "master" logs are the following:

```
ERR001 Source 'trado1' link timed out. Closing port.
   ERR### Can't connect to "DK_dialstring" for Source.
```

See “incon Log” (p. 10-29) “master Log” (p. 10-25) , “lnkpm Log” (p. 10-31) , and “Administer Silent Link Failure Detection” (p. 5-53) for information on these logs.

5 Other ways to verify link integrity with Find and Compute.

- Run a find on CFIMs for yesterday's date:
- Run compute on FDCs: **`compute row=fdc`**

  Important! It is also good to make sure that you have a good mix of fdcs on a per-switch basis. The mix should be obvious from the **`compute`** command listed above on **`row=re,fdc`** .

  For 8925 Integrated Service Assurance (ISA), for example, this verifies that the pattern file is appropriate. For a CP, for example this verifies that the FHC databases on the CP are correctly defined. If there is not a good mix of FDCs, you should have the pattern files or databases verified.

END OF STEPS

Historical Link Status

Overview

Historical link status is an optional feature that allows NTP to store and summarize historical information about each link. This information can be used to analyze the reliability and data rate of each link over a wide time period.

Storage of Historical Information

When the Historical Link Status feature is enabled, the system begins storing 5-minute link status information in the linkhist table. The data from the previous day is summarized for each source RE pair and stored in the linksum table on a daily basis.

- The linkhist table contains all link status information for the previous 8 days
  The linksum table contains summarized data for the previous 35 days. Each record contains the following information about each source RE pair:
  - Average data rate for the day
  - Peak data rate for the day
  - Number of 5 minute intervals the link was degraded
  - Number of 5 minute intervals the link was down
  - Number of 5 minute intervals the link state could not be determined.

Viewing Information

To view this information:

- On the BB-GUI — use Find > linkhist or Find > linksum and then run a Compute for a more in-depth analysis.
- From the command line — **`use sui find source=linkhist or sui find source=linksum`**.

Enabling and Configuring Source Groups

Source Groups Feature

If purchased, the Source Groups feature enables you to have multiple REs with the same name on different sources.

Example:

Without this feature, if REs A, B, and C reside on sources 1 and 2, and RE A goes down, RE A is considered down on both sources and thresholds are not updated.

With the Source Groups feature, if RE A is down on one source but up on another, NTP considers it to be up and thresholds are updated.

Enabling Source Groups

When the Source Group feature is enabled, any source groups that already exist will begin working with the feature automatically.

Configuring Source Groups

To configure a new source group:

1. Set up the RE to come into NTP on multiple sources.
2. Configure your mediation system to forward from multiple sources in the event of failure.

6 Add or Delete Users

Overview

Purpose

This chapter provides the procedures to add and delete system users. Adding a user gives that person access to the user interface (see also "User Interfaces" (p. 1-5) and "BB-GUI client software components" (p. 6-60)). The access users have to Network Trouble Patterning software depends on how you add them to the system.

- The BB-GUI (browser-based graphical user interface) is the normal NTP interface for analysts.
- NTP administrators need to access the SUI (command line) interface.

Reference: To modify attributes for an existing user, see Chapter 7, "Modify Users".

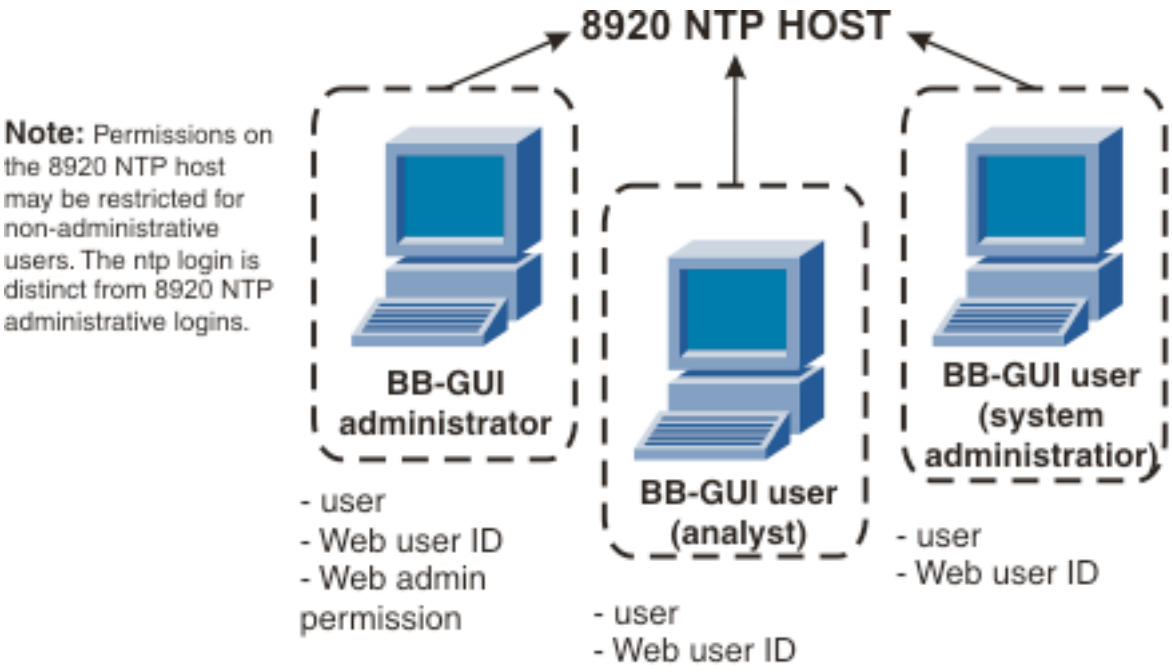
Contents

Introduction

Task Overview

Illustration

This illustration shows the relationship between how users are administered and their permissions to use the system and interfaces.



List of tasks

This table lists the tasks, procedures, and guidelines for adding and deleting NTP users IN THE ORDER they are typically done.

The table shows the relation between the procedures and the interface(s) users can access.

Access	Task order	Description	Procedures and guidelines
Add users			

Access	Task order	Description	Procedures and guidelines
UNIX	"Add a User Login ID on the NTP Host" (p. 6-8)	UNIX users need a login on the host computer where NTP runs. A user's host login must exist BEFORE you can add him or her to NTP.	Use standard administrative procedures for your operating system, but see "Create a host user ID" (p. 6-10) for guidelines.
all and BB-GUI (Use either method)	"Add an NTP user" (p. 6-22)	Use the **`add_ntpuser`** command to add the user to NTP. The attributes file read by this command sets user attributes. This also creates a BB-GUI user with like user attributes.	"Add an NTP user" (p. 6-22)
	"Add a BB-GUI user" (p. 6-54)	Use the Web User Information page to make the NTP user a BB-GUI user, and Install the client software on the user's PC. This also creates an NTP user with like user attributes.	• (includes several subprocedures to set user attributes for the BB-GUI) • "Install Client Software for the BB-GUI" (p. 6-62)
SUI	Set up user access	You must set up a way for users to access the SUI interface. You can configure remote access through a customer-provided PC X-emulation tool	(SUI) Follow local practices for remote access to host systems.
BB-GUI	Set up user access	Your NTP support organization will have set up web service on your network for the BB-GUI when the system was installed.	
all	Explain NTP access to users	Inform users how to access the interface(s) for which you have administered them.	"BB-GUI client software components" (p. 6-60)
Delete users			

Access	Task order	Description	Procedures and guidelines
BB-GUI and all (Use either method)	"Delete BB-GUI Users" (p. 6-55)	Use the user's Web User Information page to delete the user, and uninstall the client software from the user's PC. This also deletes associated NTP user.	• "Delete BB-GUI Users" (p. 6-55) • "Uninstall Client Software for the BB-GUI" (p. 6-71)
	"Delete an NTP user" (p. 6-30)	Use the **`del_ntpuser`** command to remove the user from NTP (see "Delete an NTP user" (p. 6-30)). This also deletes associated BB-GUI user.	"Delete an NTP user" (p. 6-30) Note that if the user is also to be deleted from the NTP host, use standard operating system procedures to do so.

Add and Delete NTP Users

Overview

Purpose

This section explains how to use the following NTP commands to add and delete NTP users:

- Add — "add_ntpuser Command" (p. 6-25)
- Delete — "del_ntpuser Command" (p. 6-32)

Add

The **add_ntpuser** command can only be run by the **ntp** login.

- The new ID can be set up to run either a BB-GUI interface or a UNIX shell (or both).
- A UNIX user does not need to be associated with a BB-GUI user and vice versa. There may be a UNIX user ID and a BB-GUI user ID having the same value, and then this user is both a UNIX user and a BB-GUI user and identified to the NTP system as such. Apart from it, the user may be associated with only the UNIX or BB-GUI interface.

Delete

The **del_ntpuser** command takes away a user's access to NTP and the BB-GUI, but does not affect the user's operating system login ID.

To completely remove users from the NTP host, you must remove their login IDs through standard administrative procedures for your operating system.

Contents

Add a User Login ID on the NTP Host

Purpose

Before you can add a NTP user, you must create a login ID for the UNIX user on the NTP host.

Note: UNIX IDs only need to be created for UNIX users.

Important! If the host is in a host pair for the RDS (reference data synchronization), use this procedure twice to add the user to both hosts in the pair, with identical login ID and permissions. See Chapter 12, “Reference Database Synchronization (RDS)”.

root and ntp login ID's

The operating system root login and the NTP administrative login (**ntp**) are installed with the system. Do NOT attempt to add or delete these logins.

User shell assignment

The operating system shell you assign to a new user depends on what kind of system access they need.

User type	Access required	Shell (/etc/passwd file)
administrator	Administrators do such tasks as add and delete NTP users, modify reference data, and monitor NTP errors logs. Administrators use: • SUI commands • Operating system commands There may be only one NTP administrator at your site (the **ntp** login), or you may give other logins administrator permission.	Your system's typical POSIX shell such as: • On Sun systems: */bin/ksh* Please note that the **ntp_start** and **ntp_stop** commands are restricted to the **ntp** login. Not even the **root** login can run these commands.

User type	Access required	Shell (/etc/passwd file)
analyst	It is assumed that analysts should only use the BB-GUI, therefore they: • Do not use SUI commands • May not need to use operating system commands However, an analyst could have a UNIX account and run SUI commands. **Note:** Normally, if an analyst needs SUI or operating system access, you should add him or her as an NTP administrator, NOT as an analyst.	**Note:** BB-GUI users who are not also UNIX users do not use shell. For analysts who also have a UNIX account, their system's typical POSIX shell such as: • On Sun systems: */bin/ksh*
Restricted- (ftp logins)	**Note:** The restricted flag on a user can sometimes be used in relation with BB-GUI users (depending on the regulations. This is handled through netgroups and the restricted flag. A restricted user ID is normally set up for an ftp login, (where an ftp process writes to a user directory). Restricted users do not need to access an NTP interface or to run ANY NTP commands. Please note that some procedures to add a data source to NTP require you to set up a restricted ftp login. See "Add a Source for a Configurable Conversion" (p. 5-42).	Follow local practice and use standard administrative procedures for your operating system to assign a restricted shell. **Note:** */etc/shells*.The shell you assign may need to appear in the */etc/shells* file. See the documentation for your operating system and ftp. For security, you may need to list ONLY this shell in */etc/shells*.

Create a host user ID

Purpose

Important! This applies only to UNIX users.

Use standard administrative procedures for your operating system to add the user ID and login. For example you may use the admintool for *Sun* systems. Use the guidelines in the following table:

User	Guidelines
home directory	Create the *u s e r* as /home/*u s e r*. (For NIS networks, you may see this as /export/home/*u s e r*.)
shell	See "User shell assignment" (p. 6-8) for information on the appropriate operating system shell to assign.
password	End users do not typically need shell access on the NTP host. To restrict users from free system access, you can assign a password of *NP* in the /etc/passwd file. The user will have permission in the Oracle database, but will not be able to log on the host to run any commands. Another way to restrict access is to assign users to specific command groups that prevent them from running **`sui`** commands or NTP commands like **`dbedit`**. (Command groups are not supported on the BB-GUI.) See "Manage Command Groups" (p. 7-7).
.profile	New UNIX users need to have their **`.profile`** modified. Once a UNIX user has been created by the **`ntp`** administrator with **`add_ntpuser`**, that user needs to log into the system and execute **`/lucent/ntp/snas/appl/bin/mod_userprof`**. The **`mod_userprof`** makes sure that there is a writable **`$HOME/.profile`**, creates a **`.profile`** if necessary, and then adds the following to the end of the **`$HOME.profile`**: **`. /lucent/ntp/snas/appl/bin/u_profile`**.
login and ID	Be sure the user has a unique login and ID on the NTP host. For the login to be made an NTP user, it MUST be 1 to 8 lowercase alphanumeric or "-" characters
group	You can assign the user to any user group. You may wish to assign all users who perform like functions to the same user group. See information on the group attributes file in "Custom user and group attributes files" (p. 6-11). But this is optional, and there is no required relationship between the operating system group assignment and group attributes.

Attributes File for add_ntpuser Command

Overview

The add_ntpuser command reads an attributes file to set parameters for the NTP user it creates. You can:

- Use the system default attributes settings (see "Default attributes file" (p. 6-12)
- Modify the default attribute settings (see "Modify the default attributes file" (p. 6-19))
- Specify a custom default file for an individual user or a groups of users (see "Create a custom attributes file" (p. 6-20))

Default attributes file

- Template — *$MODELDIR/uadmin/def_attributes*
  NTP is installed with a template attributes file in the $MODELDIR directory.
- Working copy — *$USERDIR/uadmin/def_attributes*
  A copy of the template is installed in the *$USERDIR/uadmin* directory as the default. The **add_ntpuser** command reads the default file unless you specify a custom attributes file. You can modify the attributes in the default file and use your modified copy as the default.

Custom user and group attributes files

The **add_ntpuser** command lets you use custom attributes files instead of the default. These files MUST be in *$USERDIR/uadmin* and be named as follows:

- Group — grp_groupname_attributes
  where groupname is any name (**-g** option to **add_ntpuser**):
- User — user_username_attributes
  where username is the user's operating system login ID (**-l** option to **add_ntpuser**):

Order of precedence for attributes files

When **add_ntpuser** runs, the user file overrides the group file, and the group file overrides the default file. That is, **add_ntpuser** sets user attributes as follows:

1. If a user_username_attributes file resides in *$USERDIR/uadmin* where username matches the user's login ID, specified with the -l option, **add_ntpuser** reads it.
   - This file is read REGARDLESS of whether you use the -g option to specify a group attributes file.
   - If any other user attributes files reside in *$USERDIR/uadmin* , **add_ntpuser** ignores them.
2. If no matching user attributes file is present and you specify a group name with the **-g** option, **add_ntpuser** uses the corresponding grp_groupname_attributes file.
3. If you do not specify a group file and there is no matching user file, **add_ntpuser** reads the default file, def_attributes.

   Important! The groupname does NOT have to match the operating system group to which the user's login ID belongs You may wish to assign operating system group membership to track with NTP group attributes, but this is not required.

Use default attributes for BB-GUI users

Certain attributes set with **add_ntpuser** also affect the BB-GUI - they are set as default values there. BB-GUI default attributes can be changed on the Web User Information page (see “Web User Information Page” (p. 6-46)).

However, you must first add all users to NTP using the procedures in this section in order to set the *Oracle* database permissions, NTP environment, and other elements for the user. Then proceed with “Add a BB-GUI user” (p. 6-54) .

Important! Use the default attributes file (def_attributes) to add BB-GUI users to NTP.

Default attributes file

The default attributes file, def_attributes, contains the following lines.

Reference: See “Attributes for add_ntpuser” (p. 6-14) for a complete description of each attribute.

```
#!/usr/bin/sh

##This file contains default definitions

#Default tablespace for this user

DEF_ORA_TBLSPACE=usr

#Temporary tablespace for this user

TMP_ORA_TBLSPACE=temp

#Enter a valid FDC group

FDCGROUP=

#Enter a valid network group or segment

NETGROUP=

#Enter a valid command group

CMDGROUP=allcmds

#Is this user a restricted user

RESTRICTED=n

#Enter commentary for the user in

#up to 30 printable characters

#(excluding characters : and ').

COMMENT=" "

#Specify an existing user login upon which to base environment
  defaults.

#If no value specified, system defaults will be used.

#Environment defaults include: output formats, find command,

#option settings, search matrix formats, history, etc.

ASEXISTINGUSER=
```

```
ASEXISTINGUSER=
```

Attributes for add_ntpuser

This table explains the functions of the attributes set with the add_ntpuser command (see "Default attributes file" (p. 6-12) for an example of a attributes file that add_ntpuser reads).

Attribute	Description
DEF_ORA_TBLSPACE	Defines the user's Oracle tablespace. Default: usr
TMP_ORA_TBLSPACE	Defines the user's temporary Oracle tablespace. Default: temp
FDCGROUP	For a BB-GUI user or an administrative (SUI) user, accept the default of **all** (null attribute). Assigns the user to an FDC group. **Values** : Any group defined in the fdcgroup table (see "Create an FDC group" (p. 7-19)) or null (blank), which means **all** FDC groups. **Default** : The group defined by the FDC_GROUP variable (see "Reprocess CDRs" (p. 10-42)). When NTP is installed, the default is all FDC groups. • **BB-GUI** . This attribute applies to SUI users. However, it also affects FDC group access in the BB-GUI. It is possible to change this default value of FDC group access directly on the Web User Information page. • "**all** ". There is no FDC group called "all". You do NOT need to create one. • **User self-reassignment** . If you assign a group, make a note that IF the user needs to switch to any other group, you must use "Change user FDC group (mod_fdcgrp)" (p. 7-25) to give the user permissions for those groups. • **sysuser table** . The group you select is entered in the fdcgroup field in the "sysuser Table" (p. A-157) . If you select all by leaving this attribute blank, a value of - is entered into the sysuser table. Please note that if you assign the user to all FDC groups, you can NOT restrict the user (see the RESTRICTED attribute below).

Attribute	Description
NETGROUP	For a BB-GUI user or an administrative (SUI) user, accept the default of **all** (null attribute). Assigns the user to a network group or segment. **Values** : Any group defined in the netgroup table OR netseg table (see "Define Network Groups and Segments" (p. 7-34)) or null (blank), which means **all** network groups and segments. **Default** : Null (the group defined by the NET_GROUP variable — see "Reprocess CDRs" (p. 10-42)). When NTP is installed, this default is null, which allows the user to switch among ALL network groups and segments. • **BB-GUI** . This attribute applies only for SUI users and does not affect the BB-GUI, for which network group and segment access is assigned SEPARATELY. Nonetheless, you must define an attribute to add the user. • "**all** ". There is no network group or segment called "all". Do do NOT need to create one. • **User self-reassignment** . If you assign a group (or segment), make a note that IF the user needs to switch to any other group or segment, you must use "Change user network group (mod_netgrp)" (p. 7-44) to give the user permissions for those groups. • **sysuser table** . The group you select is entered in the netgroup field in the "sysuser Table" (p. A-157) . If you select all by leaving this attribute blank, a value of - is entered into the sysuser table. Note that if you assign the user to all network groups and segments, you can NOT restrict the user (see the RESTRICTED attribute below).

Attribute	Description
CMDGROUP	For a BB-GUI user or an administrative (SUI) user, accept the default of **allcmds** . Assigns the user to a command group. **Values** : This group must be defined in the cmdgroup table (see "Create a command group" (p. 7-10)). **Default: allcmds** , which giver the user access to all NTP commands. • **BB-GUI** . This attribute applies only for SUI users and does not affect the BB-GUI. BB-GUI users execute pages rather than commands. Nonetheless, you must define an attribute to add the user. • **allcmds** . We recommend you do NOT redefine the allcmds group, which is prepopulated in the cmdgroup table when your system is installed. • **sysuser table** . The group you select is entered in the cmdgroup field in the "sysuser Table" (p. A-157) .

Attribute	Description
RESTRICTED	Normally, for a BB-GUI user or an administrative (SUI) user, accept the default of **n** . Determines whether the user can switch among FDC groups and among network groups and segments. **Values: y** (yes, restricted) or **n** (not restricted). **Default: n** . Typically you will enter **n** to enable the user to switch among all FDC groups and network groups and segments. You will probably use **y** only for a person external to your company. • **BB-GUI** . The restricted flag on a user can also be used in relation with BB-GUI users. This is handled through netgroups and the restricted flag. • **Restricted users** . A restricted user sees and can access: – The FDC group you assigned with the FDCGROUP attribute, plus any groups you give permission for in the fdcpermit table.(see "Change user FDC group (mod_fdcgrp)" (p. 7-25)) PLUS – The network group or segment you assigned with the NETGROUP attribute, plus any groups and segments you give permission for in the netpermit table (see "Give user network group or segment permission" (p. 7-45)) • **Unrestricted users** . An unrestricted user sees and can access "all" as a choice for both FDC groups and network groups and segments IN ADDITION to the choices assigned with the FDCGROUP and NETGROUP attributes and in the fdcpermit and netpermit tables. Making a user unrestricted effectively overrides his or her assignment for FDC groups and network groups and segments. • **Not for command groups** . This attribute does NOT affect command group access. • **sysuser table** . The value (y/n) you select is entered in the restricted field in the "sysuser Table" (p. A-157) .

Attribute	Description
COMMENT	Lets you enter a comment for this user, such as role, location, responsibility, and so forth. **`Values`** : Up to 30 alphanumeric characters, excluding colon (:) and single quote ('). **`Default`** : Null (no comment). • **`BB-GUI`** . This attribute applies to SUI users. However, it also affects FDC group access in the BB-GUI. It is possible to change this default value of FDC group access directly on the Web User Information page. **Reference:** See BB-GUI User's Guide, Web User Information and Administration for more information on the Web User Information page. • **`sysuser table`** . This value is entered into the name field of the "sysuser Table" (p. A-157) .
ASEXISTINGUSER	For a BB-GUI user or an administrative (SUI) user, you typically accept the default of null (no entry). Lets you specify an existing NTP user on which to base the new user's environment settings, such as output formats, option settings, search matrix formats, history, etc. **`Values`** : Login ID of an existing user. **`Default`** : No entry (use the defaults).

Modify the default attributes file

Purpose

You can modify the default attributes file ($USERDIR/uadmin/def_attributes) for your installation.

- Use a text editor (such as vi) to change the attributes, as needed.
- If you need to return to the system default attributes file, copy it from $MODELDIR/uadmin to $USERDIR/uadmin.

Reference: See "Attributes for add_ntpuser" (p. 6-14) for specific information on values for the various attributes.

Create a custom attributes file

Purpose

Use this procedure to create a custom attributes file.

1 Copy the $MODELDIR/def_attributes template file (or any other attributes file previously created in $USERDIR/uadmin) to another filename. To create:

- A group attributes file to be used for any users, copy the file to the following filename in $USERDIR/uadmin:

  grp_*groupname*_attributes
  where *groupname* is any name.
- An attributes file for a specific user, copy the file to the following filename in $USERDIR/uadmin:

  user_*username*_attributes
  where *username* is the user's login ID on the NTP host.

2 Use a text editor (such as **vi**) to change the attributes, as needed.

Reference: See "Attributes for add_ntpuser" (p. 6-14) for specific information on values for the various attributes.

END OF STEPS

Add NTP Users

Purpose

This procedure creates an NTP user from a login on the NTP host. The user then can have access to the system interfaces, such as either the UNIX interface or BB-GUI interface, or both.

Note: A UNIX user does not need to be associated with a BB-GUI user and vice versa. There may be a UNIX user ID and a BB-GUI user ID having the same value, and then this user is both a UNIX user and a BB-GUI user and identified to the NTP system as such. Apart from it, the user may be associated with only the UNIX or BB-GUI interface.

Important! If the host is in a host pair for RDS, use this procedure twice to add the user to both hosts in the pair, with identical login ID and permissions. See Chapter 12, "Reference Database Synchronization (RDS)".

Before you begin

- Host login. A login must exist on the NTP host for the NTP UNIX user you want to create (see "Add a User Login ID on the NTP Host" (p. 6-8) for guidelines). If the UNIX user's login ID does not exist on the host, you see the following message:

  User user not defined

  Add the user on the NTP host, and return to this procedure.
- add_ntpuser command. This procedure uses the add_ntpuser command on the login ID of a user who already exists on the NTP host. See "add_ntpuser Command" (p. 6-25) for a complete description of add_ntpuser options.
- Attributes file. You can specify a custom group or user attributes file, which must reside in the $USERDIR/uadmin directory when you run add_ntpuser (see "Attributes File for add_ntpuser Command" (p. 6-11)). However, you can run add_ntpuser from any directory.

Add an NTP user

Purpose

Use this procedure to create an NTP user from a host login.

1 Log on the NTP host.

Important! add_ntpuser is run by **ntp** , not **root** .

2 Enter
add_ntpuser -i ID -c -u [-*b* or -w] [-f fdcgroup] [-n netgroup] [-a <e-mail>]

Where:

- *ID* is the user's login ID/WebID on the NTP host/BB-GUI, must begins with a letter
- -*u* Indicates UNIX user
  Note: -*u* can be used with either -*b* or -*w* , or alone.
- -*b* Indicates BB-GUI normal user
  Note: -*b* and -*w* are mutually exclusive.
- -*w* Indicates BB-GUI admin user
  Note: -*b* and -*w* are mutually exclusive.
  Note: -*w* can't be used with option -*r* together at the same time.
- -*f fdcgroup* Allows to set up fdcgroups.
- -*n netgroup* Allows to set up netgroup.
- -*a <e-mail>* Defines an email address for a bbgui user

You can specify a custom attributes file, if desired:

- To set custom group attributes, use the **-g groupname** option to specify a grp_*groupname* _attributes file in $USERDIR/uadmin.
- To set first and last names, use respectively **-F <first name>** and **-S <last name>** parameters.
- Use **-P <BB-GUI password>** option to set BB-GUI password. For reference, see "add_ntpuser Command" (p. 6-25).
- Use optional **-r** parameter to indicates a restricted user.
- Use **-e** option to force user to select new password at first login.
- To set custom individual attributes, make sure a user_*ID* _attributes file resides in $USERDIR/uadmin.

  Important! If you see the following message, use the **-h /home_directory** option to the command.

User home directory does not exist

Example: This example for user johndoe uses a group (analyst)attributes file, and asks for confirmation. (See the examplesin "Delete an NTP user" (p. 6-30) for more information.)

add_ntpuser -i johndoe -g analyst -c

Result: (If you did not use the **-c** option, go to the response in Step 5.)

The NTP attributes that will be set for this user are displayed, followed by a prompt to abort (a) or continue (c).

```
User: johndoe
Comment:
Login used as template:
Command group: allcmds
FDC group:
Network group:
Restricted user: n

Create user or Abort the add_ntpuser command? (c or a)
```

3 Check the attributes, and if they are:

- Correct, go to the next step.
- Incorrect, enter **a** to abort. Return to the beginning of this procedure.

4 Enter **c** to continue.

Result: You see a series of messages, including the following:

```
Creating Oracle account for user
Setting application environment for user
PRM configured from file: /etc/prmconf [list of PRM users]
```

When the user has been successfully added, you see the following message:

```
User user added to Oracle and <application> successfully.
```

5 **Important!** This step applies only to UNIX users.

Ensure that the user's .profile has been updated appropriately.

Once a UNIX user has been created by the **ntp** administrator with **add_ntpuser** , that user needs to log into the system and execute **/lucent/ntp/snas/appl/bin/mod_userprof** . The **mod_userprof** makes sure that there is a writable **$HOME/.profile** , creates a **.profile** if necessary, and then adds the following to the end of the **$HOME.profile** :
. /lucent/ntp/snas/appl/bin/u_profile .

6 Will the user access NTP exclusively through the BB-GUI?

- If YES, do the following:
  - Tell the user his or her Web User ID and password. The BB-GUI password defaults to **<welc0me!>** .
  - Tell the user how to access NTP. Use "BB-GUI client software components" (p. 6-60) for reference.
- If NO, go to the next step.

7 Use this checklist to determine what else to do to configure the user.

- Did you assign the user to an FDC group other than *all* , and will the user need to switch to other groups?
  If YES, see "Change user FDC group (mod_fdcgrp)" (p. 7-25) to give the user permission for other groups.
- Did you assign the user to a network group or segment other than *all* , and will the user need to switch to other groups and segments.
  If YES, see "Give user network group or segment permission" (p. 7-45) to give the user permission for other groups and segments.
- Tell the user his or her NTP host login and password and choices for command groups, FDC groups, and network groups and segments.

END OF STEPS

add_ntpuser Command

Purpose

The add_ntpuser command creates an NTP user associated with either the UNIX or BB-GUI interface, or both.

Things to remember

- add_ntpuser is run by **ntp**, not **root**. **Root** is only used to create and delete UNIX accounts. Normal operations are all run by **ntp**.
- Due to not having **root** authority, after creating a UNIX user, the user needs to run **mod_userprof** to modify their profile.
- While creating an NTP user, remember that a UNIX user does not need to be associated with a BB-GUI user and vice versa. There may be a UNIX user ID and a BB-GUI user ID having the same value, and then this user is both a UNIX user and a BB-GUI user and identified to the NTP system as such. Apart from it, the user may be associated with only the UNIX or BB-GUI interface.

  Important! UNIX only users cannot be managed from BB-GUI side. Use *dbedit* to manually update *fdcpermit* and *netpermit* tables to assign FDC and NET groups to restricted user. This procedure of assigning of FDC and NET groups is valid only for UNIX users. To assing FDC and NET groups to BB-GUI users use Group manager, for more information see “Group Manager” in BBGUI User's Guide.

Description

The add_ntpuser command reads an attributes file in the **$USERDIR/uadmin** directory and uses the parameters defined there to configure the new user. See “Attributes File for add_ntpuser Command” (p. 6-11) for a complete description of the attributes. This command also sets up the user's:

- NTP environment
- Oracle database account and permissions

Modifying New UNIX User's .profile

Once a UNIX user has been created by the **ntp** administrator with **add_ntpuser**, that user needs to log into the system and execute **/lucent/ntp/snas/appl/bin/mod_userprof**. The **mod_userprof** makes sure that there is a writable **$HOME/.profile**, creates a **.profile** if necessary, and then adds the following to the end of the **$HOME.profile**: **. /lucent/ntp/snas/appl/bin/u_profile**.

Syntax

```
add_ntpuser -i ID [-c] [-g groupname] [-u] [-r] [-b] [-w] [-F
<first name>] [-S <last name>] [-P <password>] [-e] [-f
fdcgroup] [-n netgroup] [-a <e-mail>]
```

Parameter	Description
-i ID	(required) Identifier associated with this NTP user for both Unix and BB-GUI Web ID. When the command executes, an entry is made for this user in the sysuser table. Must begins with a letter. **Note:** For UNIX users, remember that before you can add an NTP user, you must create a login ID for the user on the NTP host (see "Add a User Login ID on the NTP Host" (p. 6-8)). Please note that if a user_**ID**_attributes file resides in $USERDIR/uadmin (where **ID** is the login ID), **add_ntpuser** uses this file to set the user's attributes, regardless of whether you use the **-g** (group) option below.
-g groupname	(optional) Specifies a group, which causes **add_ntpuser** to use a custom group attributes file, called grp_**groupname**_attributes, if one exists. • The grp_**groupname**_attributes file MUST reside in $USERDIR/uadmin. • If a user attributes file exists for this user (see the **-l** option above), **add_ntpuser** will use it instead, and ignore the group attributes file. • **groupname** must match **groupname** in the grp_**groupname**_attributes filename. See "Attributes File for add_ntpuser Command" (p. 6-11) for more information.
-c (confirmation)	(optional but recommended) Displays NTP attributes that will be set for this user, and allows you to confirm them before the user is actually added.
-u	(optional) **-u** Indicates a UNIX user.
-r	(optional) **-r** Indicates a restricted user. **NOTE:** This option is available only if NETSEG feature is enabled in the NTP. To enable this feature conntact your Alcatel-Lucent Customer Engineer.

Parameter	Description
-b **-w**	(optional) **-b** Indicates BB-GUI normal user. **-w** Indicates BB-GUI (web) admin user. To create a BB-GUI user, either **-b** or **-w** must be specified. If none are specified, a BB-GUI user login **is not created**. **Note:** the *-w* option can't be used together with *-r* option.
-F <first name>	(optional) User's first name. This field defaults to the login id.
-S <last name>	(optional) User's last name. This field defaults to the login id.
-P <BB-GUI password>	(optional) User's BB-GUI password. This field defaults to **<welc0me!>**. The password must be at least 8 characters long. For initial passwords, please refrain from using special characters that can be interpreted in the command line. The following characters may be interpreted incorrectly: (){}[]<>$#^*& When a new user is added with the default password, during the first access to the bbgui the <welc0me!> password has to be used. Immediately after login user will be sent to a new page to enter a new password (and verify) and then will be sent back to the login dialog to log in with the new password again.
-e	(optional) Expires initial password at first user login. Forces user to select new password. Default, if a new user is added with the default password.
-f fdcgroup **-n netgroup**	(optional) **-f** Allows to set up fdcgroups. **-n** Allows to set up netgroups. These parameters used with the **add_ntpuser** command allow for setting up the **fdcgroup** and **ntpgroup** attributes while adding new NTP users. Note that these attributes are also set up for the BB-GUI users. **Note:** The **-f** and **-n** parameters overwrite the settings in the default attributes file. **Example:** **add_ntpuser -i username -w -P ****** -n nettest1, nettest3,segtest3,segtest2 -f fdctest1,fdctest2, fdctest3**
-a <e-mail>	(optional) Defines an email address for a bbgui user

Example:

- This command makes the NTP host login johndoe an NTP user and a BB-GUI normal user with the default user attributes from the **def_attributes** file.
  add_ntpuser -i johndoe -b -a johndoe@alcatel-lucent.com
- These commands prompt you for confirmation before making NTP host login johndoe an NTP user with custom attributes.
  – Uses a group attributes file named **grp_analyst_attributes**
  add_ntpuser -i johndoe -g analyst -c
  – Uses a user attributes file named **user_johndoe_attributes.**
  add_ntpuser -i johndoe -g johndoe -c

Delete NTP Users

Purpose

This procedure removes a user's access to NTP (including the BB-GUI). For why you would delete an NTP user, see "List of tasks" (p. 6-3).

Important!

- To completely remove the user from the NTP host, you must also remove the user's login ID. Use standard administrative procedures for your operating system. See your operating system reference documents, if necessary.
- If the host is in a host pair for RDS (reference data synchronization), use this procedure twice to delete the user from both hosts in the pair. See Chapter 12, "Reference Database Synchronization (RDS)".

Before you begin

`del_ntpuser` command. This procedures uses the del_ntpuser command on the login ID of the NTP user. See "List of tasks" (p. 6-3) for a complete description.

Delete an NTP user

Purpose

Use this procedure to remove NTP access for a login ID on the NTP host.

1 Warn the user to be deleted that all his or her working sets (user files) will be deleted.

Important! The files in the user's home directory will NOT be affected.

2 Log on the NTP host.

Important! **`del_ntpuser`** is run by **`ntp`** , not **`root`** .

3 Enter **`del_ntpuser -i`** ***`ID`*** **`[-c]`**

Where:

- *`ID`* is the user's login ID/WebID on the NTP host/BB-GUI
- `-c` Confirms action(s) prior to execution

Result: (If you did not use the **`-c`** option, go to the response in *Step 4* .) You are prompted to confirm the deletion, as follows:

```
User:  user

WARNING: All tables for user
 will be removed.
Delete user
 or Abort the del_ntpuser command? (d or a)>>
```

4 Enter **`d`** to delete the user.

Result: You see output resembling the following as the user is removed.

```
User dropped.

User user
 dropped from Oracle
[a list of rows deleted]
[a list of users]

PRM application manager state: Enabled (polling interval: 30
   seconds)


Disk manager state: Disabled
User user
 deleted from Oracle and <application>
 successfully
```

END OF STEPS

del_ntpuser Command

Purpose

The **del_ntpuser** command removes a user from NTP. It takes away the user's:

- Oracle database account and permissions
- Access to the NTP user interfaces
- NTP environment variables
- Working sets (user files)

However, **del_ntpuser** does not remove the user's:

- NTP host login or any files in the user's home directory (See documentation on user administration for your platform for standard procedures to remove login IDs.)

  Important! Do NOT attempt to change a user's attributes by deleting and re-adding them as an NTP user. Instead, see Chapter 7, "Modify Users".

Syntax

```
del _ntpuser  -i ID [-c]
```

Parameter	Description
-i ID	(required) Identifier associated with this NTP user for both UNIX and BB-GUI Web ID.
-c (confirmation)	(optional) Prompts you to confirm that you really want to delete the user.
ID	(required) Specifies the user's login ID on the NTP host (see "Add a User Login ID on the NTP Host" (p. 6-8)). *Example:* This command removes NTP user johndoe.**del_ntpuser -i johndoe**

Add and Delete BB-GUI Users

Overview

Purpose

Background

NTP is installed with an initial BB-GUI administrator ID (NetAdmin). This ID can add other users and can give them BB-GUI web administration permission. BB-GUI web administrators can modify user information for all BB-GUI user IDs.

BB-GUI client software must be installed on users' PCs before they can run the BB-GUI. This software should be uninstalled when a client machine is taken out of service from NTP. Required software components differ depending on whether the BB-GUI runs on a PC and whether a user needs to access Pattern Painter graphical output.

Important! A new user can be added with either the add_ntpuser command (see "Add an NTP user" (p. 6-22)) or through the BB-GUI. You do not need to use both procedures. Using the add_ntpuser will automatically create a like user on the BB-GUI. Using the BB-GUI to add a user will result in a like user login being created on NTP.

Similarly, users need only be deleted using one method: del_ntpuser (see "Delete an NTP user" (p. 6-30)) or through the BB-GUI.

Task overview

Use these procedures for BB-GUI user administration tasks.

Task	Procedures
Add users	• "Add a BB-GUI user" (p. 6-54) • "Install Client Software for the BB-GUI" (p. 6-62) – "Install BB-GUI client software — PC" (p. 6-64) – "Example" (p. 6-39) – "Install Pattern Painter software — PC" (p. 6-67)
Modify users	• "Modify BB-GUI User Information" (p. 7-6)

Task	Procedures
Delete users	"Uninstall Client Software for the BB-GUI" (p. 6-71) • "Password Administration" (p. 6-35) • "Uninstall Pattern Painter client software — PC" (p. 6-74)

Reference

- For pages you use to administer BB-GUI user IDs, see "Web User Administration Page" (p. 6-38) and "Web User Information Page" (p. 6-46).
- For other tasks and procedures related to the BB-GUI, see "Modify BB-GUI Users" (p. 7-6) and "Customize the BB-GUI" (p. 9-4).

Contents

Password Administration

Overview

Defining characteristics of BB-GUI passwords can minimize unauthorized access to the system. Those with administrator/root permission can configure specific BB-GUI password characteristics for users including:

- Minimum number of characters required for BB-GUI user password. A new or modified password must contain at least the specified minimum number of characters to be considered valid. The minimum is configurable.
- Password composition. This requires a user password to contain characters from specific groups (alpha-numeric, special, etc.) to be considered valid. The character groups are configurable.
- Password Aging. This requires a user password to be changed within a given number of days. By default, the password cannot be changed for 3 days after it is issued and MUST be changed after 90 days. These defaults are configurable.

  When the user's password expires, the user will be redirected to a password modification page until the password has been modified. The number of days is configurable.

  Important! By default, any user marked as a web user administrator is exempt from Password Aging checks when modifying a password. The web user administrator can change any user's password whenever they like.
- Inactivity Lock. A user's entry is "locked" from BB-GUI access after the specified number of consecutive inactivity days is reached.
- Ineffective authentication attempts lock. A user's entry is "locked" from BB-GUI access after the specified number of consecutive failed authentication attempts is reached. The minimum value is 2.
- Temporary password assignment. This capability allows a Web User Administrator to mark a user's entry such that it will require the user to enter a new password upon its next use.

The web user inactivity and password aging checks are performed as part of the expire users (exp_usrs) script executed through the cron. Therefore, if the cron is not available at the appropriate time or the cron tables are modified to affect the execution of the log check script, the ability to accurately perform the inactivity and password aging checks may be affected.

Password Composition

The password length and composition components, by default, are set to a minimum length of 8 characters and are required to have characters from at least 3 of the 4 following sets:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
1234567890
!#^*()-_+={}[];:,./<>$&
```

Important! For initial passwords, please refrain from using special characters that can be interpreted in the command line. The following characters may be interpreted incorrectly:

(){}[]<>$#^*&

Additionally, a user's password cannot be the same as that user's ID.

The password length and composition components are configurable but can be complex to administer. Contact NTP Technical Support for assistance.

Password Expiration and Failed Authorization

If a user's password is scheduled to expire in 10 days or less, a warning will be shown before the first page is loaded to notify the user that should go to the admin page and change password. If a user's password expires, the user is redirected to a password administration screen upon his next BB-GUI access request. A new password must be entered at that time. By default, users may not use their previous 10 passwords. This default is configurable.

If a user's password is changed while they have a browser session active that had previously authenticated through the BB-GUI, their next web access attempt will result in a "retry" response. This affects all previously authenticated browser sessions for this user on all clients. Simply retry using the new password to gain access.

Exceeding the Defined Thresholds

Users trying to access the system that has exceeded a threshold may be:

- prompted to refresh their password,
- denied BB-GUI access,
- asked to re-enter a password that will conform to length or composition rules.

Excluding Users from Password Thresholds

Individuals can be excluded from the processing for the characteristics by defining those who are not to be included on the "PWA_<characteristic>_EXCLUDE<user Ids>" line of the */lucent/ntp/wgui/conf/pwa.conf* file. User Ids can be a single web user Id, or a list of web user Ids separated by "|" symbols. Do not use white spaces within the "user(s)"

string. Follow the comment text and examples given in the pwa.conf file. If no user is to be excluded, then this line must be commented out by using the "#" symbol at the beginning of the line referred to above.

Important! If the web user administrator is NOT excluded from the various thresholds, then you risk losing the capability to perform web user administration/recovery.

Modifying Passwords

To modify the password cycling, ineffective attempts, inactivity, or expiration characteristics, login as root and edit the */lucent/ntp/wgui/conf/pwa.conf* file and adjust the items which are configurable by following the commented text included. After changes are made, the web server must be restarted for the changes to take effect.

Important!

- The BB-GUI will be unavailable to all users during the period in which the web server is stopped and is restarting for the given host.
- It is recommended that a copy of the file be saved before editing to allow a recovery path in the event of server startup failure. After changes are made, the web server must be restarted for the changes to take effect.

Resetting Passwords

To reset the user's BB-GUI password once the inactivity or ineffective attempts threshold is exceeded, the Web Administrator needs to specify a new one for the user through the Web User Information Page. In addition to resetting the password the administrator may also choose to use the "expire password now" option on the Web User Information Page to force the user to select a new password upon his next NTP Web GUI access attempt.

Web User Administration Page

Purpose

The Web User Administration page lists all BB-GUI users. It allows any user with BB-GUI administration permission to

- Select an existing BB-GUI user to administer by accessing their Web User Information page
- Access a blank Web User Information page to add a new BB-GUI user

Reference: See "Web User Information Page" (p. 6-46).

Important! Only users with BB-GUI administration permission can access the Web User Administration page. When users without this permission click **Web User Administration** from the product Launch page, they are redirected to their own Web User Information page.

Go to the Web User Administration page

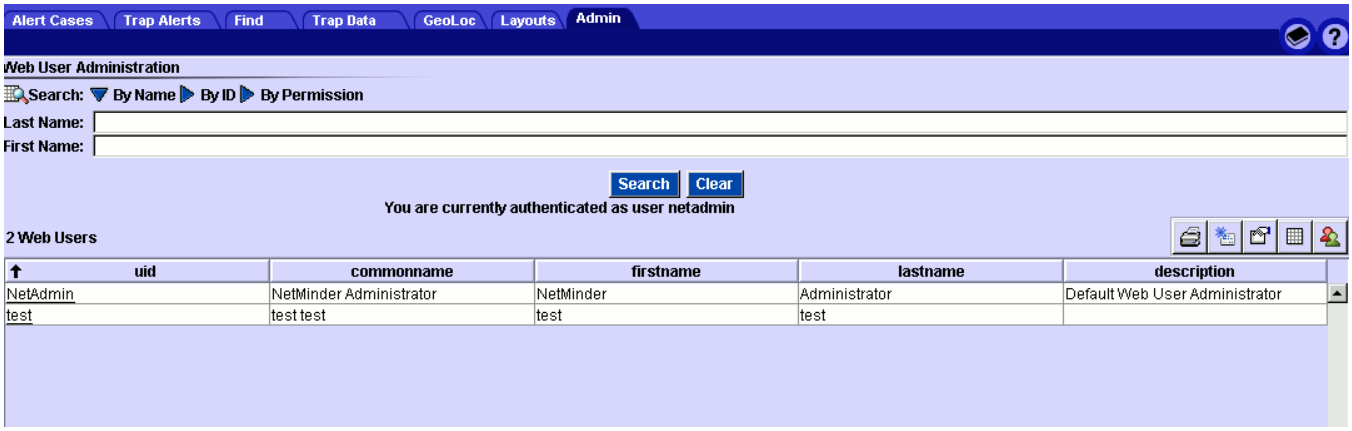
Purpose

From the product Launch page, click **Web User Administration**, and enter your user ID and password when prompted.

Reference: For information on the Launch page, see the *BB-GUI User's Guide*.

Example

Here is an example of the Web User Administration page. For a description of the page parts, see "Web User Administration page parts" (p. 6-39).



Web User Administration page parts

The Web User Administration page parts have the following functions:

Field	Description
Search	
Search Criteria	*Search area.* Click the triangle next to **By Name**, **By ID**, or **By Permission** to search for users. From the search results, you can select a user to administer. To search by: • Name — Enter the user's first name, last name, or both. For example, if you enter Bob in the First Name field, the user information for all BB-GUI users named Bob is displayed. • User ID — Enter a user's Web User ID. • Permission —Select Web Administration permission/non Web Administration permission.
Buttons Specific to the Page	

Field	Description
Search	Begin your specified search.
Clear	Clear the search fields.
Icons Specific to the Page	
	**Create a new entry in the table icon**. (Visible for NetAdmin user only.) Click this icon to display a blank Web User Information page where you can add a new BB-GUI user (see "Web User Information Page" (p. 6-46)).
	User Default icon This icon allows administrators to set defaults for: • all users • newly-defined users. See "Setting User Defaults" (p. 6-43).
	User Table icon This icon brings up the Administer User Tables screen. From this screen the administrator can view and/or delete user tables saved by any user. See "View or Delete User Tables" (p. 6-45).
	Group Manager icon This icon brings up the Group Manager dialog window. From this window the administrator can view, create, delete and edit following items: • FDC Groups • Networks Groups • Network segments For more information about Group manager, see "Group Manager" in *BBGUI User's Guide.*
Web User Information	
Web User Information	Information about user, including: • Web User ID • Common Name • First Name • Last Name • Description.

Display a blank Web User Information page

Purpose

To display a blank Web User Information page to use for adding a new user, go to the Web User Administration page and click the **create new entry in table** icon.

Reference: To access the Web User Administration page, see "Go to the Web User Administration page" (p. 6-39). For an illustration of the Web User Administration page and its parts, see "Example" (p. 6-39) and "Web User Administration page parts" (p. 6-39).

Display a user's Web User Information page

Purpose

To display a particular user's Web User Information page so you can check or modify their user information, go to the Web User Administration page and do one of the following:

- Select the user from the list of users (see "Web User Administration page parts" (p. 6-39)) on the page.
- Use the search area (see "Web User Administration page parts" (p. 6-39)) to find the user, and then click the user's Web User ID.

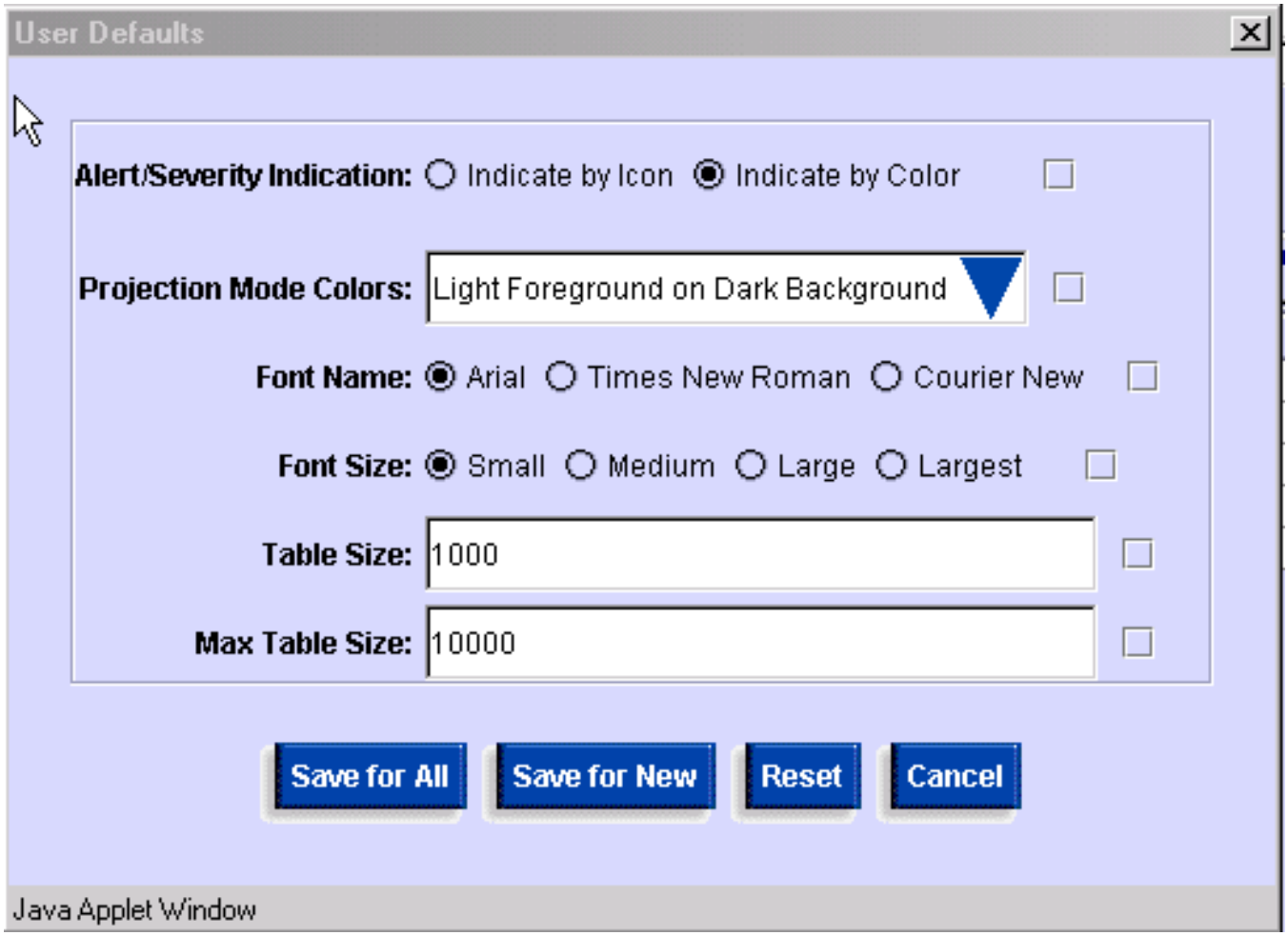
Reference: To access the Web User Administration page, see "Go to the Web User Administration page" (p. 6-39). For an illustration of the Web User Administration page and its parts, see "Example" (p. 6-39) and "Web User Administration page parts" (p. 6-39).

Setting User Defaults

Purpose

This User Defaults icon leads to the User Defaults screen (shown below). This screen allows administrators to set defaults for:

- all existing users in the system
- newly-defined users only.



Fields on the User Defaults screen are as follows:

Field	Description
Alert/Severity Indication	• Indicate by icon • Indicate by color (default)

Field	Description
Projection Mode Colors	• Light Foreground on Dark Background (default) • Dark Foreground on Light Background
Font Name	• Arial (default) • Times New Roman • Courier New
Font Size	• Small (default) • Medium • Large • Largest
Table Size	1000 (default)
Max Table Size	10,000 (default)

Enabling changes to the defaults

At the end of each row on the User Defaults screen is a checkbox. Checking this box enables the change made to the defaults. Unselecting the checkbox cancels the change to the defaults.

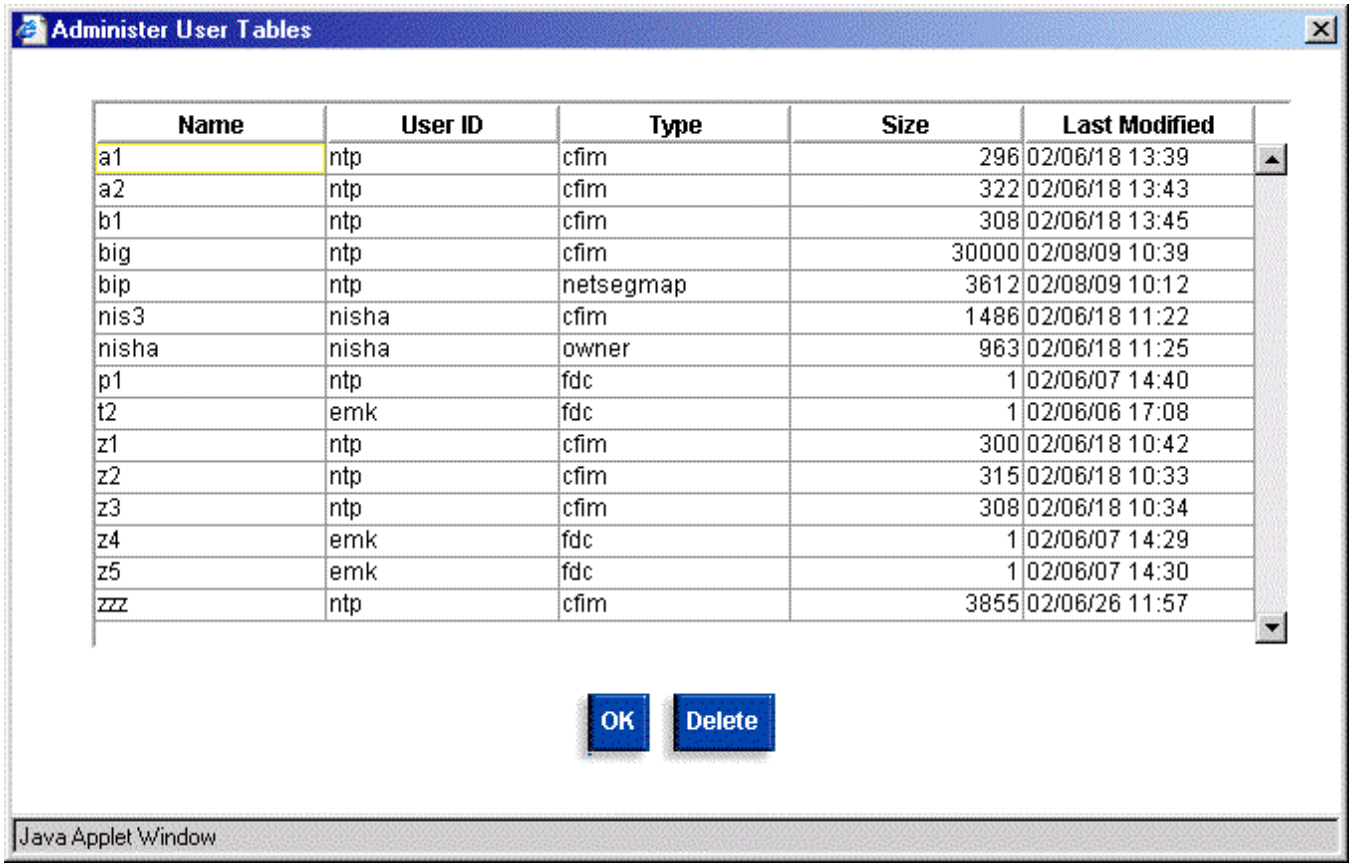
Reference: To access the Web User Administration page, see "Go to the Web User Administration page" (p. 6-39). For an illustration of the Web User Administration page and its parts, see "Example" (p. 6-39) and "Web User Administration page parts" (p. 6-39).

View or Delete User Tables

Purpose

The User Table icon brings up the Administer User Tables screen. From this screen you can view and/or delete user tables saved by any user.

This tool is useful because user table data can consume large amounts of space and you may find it necessary to delete entries to gain space in the database.



Reference: To access the Web User Administration page, see "Go to the Web User Administration page" (p. 6-39). For an illustration of the Web User Administration page and its parts, see "Example" (p. 6-39) and "Web User Administration page parts" (p. 6-39).

Web User Information Page

Purpose

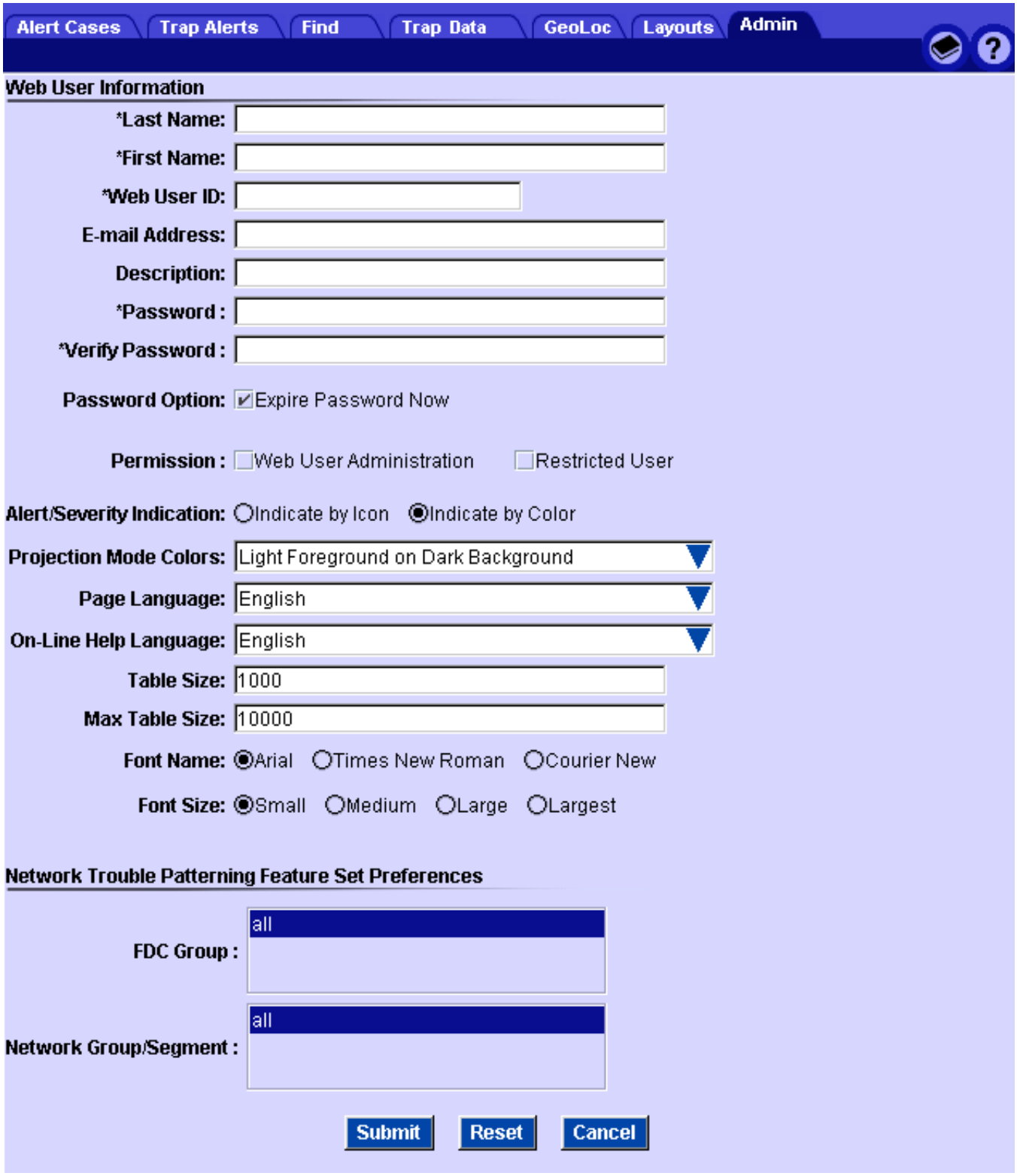
The Web User Information page is where you create and remove BB-GUI users, or modify their configuration information. The page also allows you to add E-mail addresses for scheduling Find output in the BB-GUI.

- There is a separate instance of this page for each BB-GUI user.
- A user can access his or her own Web User Information page and modify some of the information there.
- Users with administration permission can access the Web User Information pages of all other users and modify all information there except values fixed by the system.

Example

Here is an example of a Web User Information page.

Each BB-GUI user has a unique instance of this page. To add a new BB-GUI user, bring up a blank Web User Information page.


Alert Cases
Trap Alerts
Find
Trap Data
GeoLoc
Layouts
Admin
Web User Information
*Last Name:
*First Name:
*Web User ID:
E-mail Address:
Description:
*Password :
*Verify Password :
Password Option: Expire Password Now
Permission : Web User Administration Restricted User
Alert/Severity Indication: Indicate by Icon Indicate by Color
Projection Mode Colors: Light Foreground on Dark Background
Page Language: English
On-Line Help Language: English
Table Size: 1000
Max Table Size: 10000
Font Name: Arial Times New Roman Courier New
Font Size: Small Medium Large Largest
Network Trouble Patterning Feature Set Preferences
FDC Group : all
Network Group/Segment : all
Submit
Reset
Cancel

Go to the Web User Information page

Purpose

You go to this page in various ways, depending on what you want to do.

- *New users*. To access a blank Web Information Page for adding users, you simply click the button at the right side of the page (see "Web User Administration page parts" (p. 6-39)).
- *Existing users*. To access an individual user's Web User Information Page, used for modifying user information or deleting the user, either:
  - Click the user's Web User ID.
  - Use the search area to find the user, and then click the user's Web User ID.

  Reference: See "Web User Administration page parts" (p. 6-39) for information on the list of users and the page area for searching for users.

Web User Information page parts

The Web User Information page has the following areas that consist of fields in which you select or enter information.

- Web User Information area
- Preferences area

Permissions for this information are as follows:

- Any user can change values in fields with **`analyst permission`**.
- Only BB-GUI administrators can set or change values in fields with **`admin permission`**.

Some fields have a default *system value* that you cannot change.

Important!

- Fields on this page will vary depending on the features that are enabled on your system.
- See "Customize BB-GUI Attributes" (p. 9-7) for more information on default system options and values for some values in this table.

Field	Description	Permission
Web User Information		
Last Name	Contain the BB-GUI user's last and first name, respectively.	Admin
First Name		

Field	Description	Permission
Web User ID	Sets a user's web user ID. *Values*: This ID must match the user's login on the NTP host. The user may already have a BB-GUI user ID (and host login) for another product. In that case, match the BB-GUI ID here. *Add a BB-GUI Web User ID* • Type the user's name in the Last Name and First Name fields. • Type the ID in the Web User ID field. • Click **Submit**.	admin
E-mail Address	Full E-mail address for the user. This is an optional field; however, if not populated, a user will not be able to use the Scheduled Data Distribution feature. **Reference:** See *BB-GUI User's Guide* for more information on this feature.	
Description	(optional) Identifies a BB-GUI user, such as by job responsibility or location. *Assign a BB-GUI user description* • Type the description in the **Description** field. • Click **Submit**.	
Password	Used for password administration. The BB-GUI administrator initially assigns a password for new BB-GUI users. Users can change their passwords in accordance with password constraints (see "Password Administration" (p. 6-35)). *Assign a BB-GUI user password* • Type the password in the **Password** field. • Type the same password in the **Verify Password** field. • Click **Submit**.	analyst
Verify Password		
Password Option	If the Expire Password Now box is checked, the user is prompted to change their password the next time they log in. This is most often used by administrators to assign a user a temporary password.	

Field	Description	Permission
Permission	Determines whether a user has: • Web Administration permission - full administrative privileges (can change user information, etc.). *Values*: selected or unselected. *Assign BB-GUI administrator permission* • Click the checkbox to assign a user BB-GUI web administrator permission. • Click the checkbox again to unassign permission.	admin
Alert/Severity Indication	Select one of the following: Indicate by Icon, Indicate by Background Then left-click **Submit**. These choices mean: • **Indicate by Icon** — A thermometer icon is displayed in the Al (Alert Level) field. • **Indicate by Color** (default) — The background of the entire row is colored as follows: – Red — critical – Yellow — major – Cyan (blue-green) — minor Please note that the text, instead of background, is colored if you selected Light Foreground on Dark Background. *Set BB-GUI Ascreen exception level displays* • Click **Indicate by Icon** or **Indicate by Color**. • Click **Submit**.	analyst
Projection Mode Colors	To set colors, for projection mode, left-click the blue triangles to pull down menus to select from: • Dark Foreground on Light Background (default for regular mode) • Light Foreground on Dark Background (default for projection mode) After selecting from one or both menus, left-click **Submit**.	analyst
Page Language	The language for BB-GUI pages and on-line help, respectively. *Values*: English only, currently.	system value (cannot be changed)
On-line Help Language		

Field	Description	Permission
Table Size	The maximum number of scrollable rows displayed in Find at one time. This is a block of rows identified by the numbers and arrow under the bottom left corner of output. Each block is identified by numbers in the bottom left corner of output. *Values*: 5000. This parameter can be increased up to the Max Table Size number (maximum of 10,000). Please note that increasing this number will add extra wait time to load the table. *Example:* If Table Size is 5,000, and Find output indicates "15000 records found", then below the bottom left corner of output you see "1 2 3". The bold typeface means you are looking at records 1 through 5000. Click **2** to see records 5,001-10,000. Click **3** to see records 10,001-15,000.	system value (cannot be changed)
Max Table Size	The actual maximum number of records Find retrieves and Compute is done on (although at one time you can scroll only chunks of records, determined by the Table Size field). *Values*: Initial default of 10,000. Do NOT type commas between digits in this field. Please note that NTP does Computes on the whole set of records defined by the Max Table Size, not on the scrollable number of records defined by the Table Size field. *Change BB-GUI Max table size* • Type a new table size. Do NOT use commas. • Click **Submit**.	analyst
Font Name	*Change BB-GUI font name/type* Select from the following: Arial, Times New Roman, Courier New. Then left-click **Submit**.	analyst
Font Size	The font size for the display of all pages in a user's command group. *Values*: Small (12 point), medium (20 point), large (28 point), or largest (36point). *Change BB-GUI font size* • Select either **Small, Medium, Large**, or **Largest**. • Click **Submit**.	analyst

NTP Preferences

Field	Description	Permission
FDC Group	Limits output on the Alert Cases and Trap Alerts pages to only those alert cases (or CFIMs) with FDCs in the group. *Values*: FDC group(s) or all for no limits. • *Defined on host*. You define FDC groups on the NTP host (see "Create an FDC group" (p. 7-19)). The definitions affect ALL interfaces. When you administer a BB-GUI user, this field lists all groups defined. If none are defined, the only listing is *all*. • *Assigned separately*. FDC groups are assigned SEPARATELY for the BB-GUI and other NTP interfaces (SUI [administrative], and also legacy interfaces that a few customers still use). A user can have access to one set of FDC groups in the BB-GUI and to another set in the other NTP interfaces. • *Access to multiple groups*. The user can access any FDC group you assign here. The default group is the first group in the drop-down list. A user must select another group on the Web User Information page to change groups (see "Web User Information Page" (p. 6-46)). • *Override*. A user's current FDC group shows on output pages beside the page name. But using a page's search criteria overrides group settings. *Assign a BB-GUI user's FDC groups* • Click the blue triangles to pull down the menu, and select (highlight) the group(s) you want the user to be able to access. In order to select multiple groups, press **Shift** and left-click each group. • Click **Submit**. The user will see only the groups you assigned, and can select one.	analyst

Field	Description	Permission
Network Group /Segment	This field limits output to only those alert cases with those entities in the NE field, or CFIMs with those entities in the Re or De fields. • *Defined on* NTP *host*. You define network groups and segments on the NTP host (see "Define Network Groups and Segments" (p. 7-34)). The definitions affect ALL interfaces. When you administer a BB-GUI user, this field lists all groups and segments defined. If none are defined, the only listing is *all*. • *Assigned separately*. Network groups and segments are assigned SEPARATELY for the BB-GUI and other NTP interfaces (SUI [administrative], and also legacy interfaces that a few customers still use). A user can have access to one set of groups and segments in the BB-GUI and to another set in the other NTP interfaces. • *Access to multiple groups*. The user can access any network group or segment you assign here. The default group is the first group in the drop-down list. A user must select another group on the Web User Information page to change groups (see "Web User Information Page" (p. 6-46)). *Assign a BB-GUI user's network groups* • Click the blue triangles to pull down the menu, and select the group(s)/segments you want the user to be able to access. (To select multiple groups, press **Shift** and left-click each group.) • Click **Submit**. The user will see only the groups/segments you assigned, and can select one.	analyst

Add a BB-GUI user

Purpose

Use the Web User Information page to add or modify a BB-GUI user.

Important!

- Only Web Administrator can add a BB-GUI user.
- Users created from the BB-GUI that also need SUI access must have their .profile updated manually.
- System Administrator can assign a BB-GUI user to a specific command group.
- A BB-GUI user can run all the attributed commands from the assigned command group.

Procedure

Use this procedure to configure a BB-GUI user's access to NTP by adding a web user ID and user information.

1 Open a blank Web User Information page.

Reference: See"Go to the Web User Information page" (p. 6-48) for information on accessing the page.

2 Enter information in the various fields on the page.

Reference: For what to enter, see "Web User Information page parts" (p. 6-48).

3 Click **Submit**.

Result: A new BB-GUI user is added.

END OF STEPS

Delete BB-GUI Users

Overview

Use the Web User Information page to delete a BB-GUI user.

Important!

- Only Web Administrator can delete a BB-GUI user.
- After you delete a user from the BB-GUI that was created via the add_ntpuser command, the user still exists as an NTP user. To entirely remove the user, see "Delete an NTP user" (p. 6-30).

Restoring Default Searches

If an administrative user is deleted, that user's customized default searches/layouts may also be deleted (via a **y/n** prompt during the delete process). This creates a problem for other users that access those saved searches/layouts.

If this occurs, you can use the **restore_bbgui_default** command to restore the original system default saved searches and/or table layouts. You must specify "search" or "layout" to indicate which is to be restored.

```
restore_bbgui_default search or layout
```

After you enter the command, you are prompted to select a page name.

Delete a BB-GUI user

Purpose

Use this procedure to remove a user's access to the BB-GUI by deleting their web user ID and user information.

1 Go to the Web User Information page for the user.

Reference: See "Go to the Web User Information page" (p. 6-48) for the procedure.

2 Click **Delete** .

Result: A window displays the following prompt:

```
Select Yes to delete the userid or No to cancel this operation.
```

3 Click **Yes** to delete the user.

END OF STEPS

Additional User Administration Tasks

Purpose

This section provides information about additional user administration tasks, such as:

- tracking of user activity,
- broadcasting a message to all BB-GUI users, or
- allowing all users to have the same user account and password across all participating applications.

Tracking of User Activity

This feature allows the administrator to view all significant actions during operation of the web user interface, which are documented in a system log (cmdlog database table). In this way a history is maintained for each user.

Command Syntax

Viewing the contents of the log is performed using the **sui** find command.

```
sui find so=cmdlog se="owner=username" delim='";"'
```

In order to make output more readable, each record is separated by semicolon **(delim='";"')** .

Sample Output

The following is sample log output for **netadmin** .

```
sui find so=cmdlog se="owner=netadmin" delim='";"'

Seqnum;Owner;Host;Type;Command;Args;Starttime;Endtime;Status;

Completion;Error;Other;Aud_sid

FIND COMPLETED - 6 CMDLOG RECORDS FOUND

1521;netadmin;hawk8;-;find;Filter:fdcgroup=all&findtime=60,
  SearchExp:;06/04/24 09:09;-;-;-;-;-;743528

1522;netadmin;hawk8;-;find;Filter:fdcgroup=all&findtime=60,
  SearchExp:;-;06/04/24 09:10;-;Chunk completed. Records 1 through
  1000;-;-;743528

1542;netadmin;hawk8;-;ascreen;Filter:fdcgroup=all&netgroup=all,
  SearchExp:;06/04/24 09:53;-;-;-;-;-;745018

1543;netadmin;hawk8;-;ascreen;Filter:fdcgroup=all&netgroup=all,
  SearchExp:;-;06/04/24 09:53;-;Run Completed;-;-;745018

FIND COMPLETED - 6 CMDLOG RECORDS FOUND
```

Message Broadcast Feature

The Message Broadcast feature allows the administrator to broadcast a message to all BB-GUI users. This is useful in case of a system shutdown or other instance in which you need to communicate with BB-GUI users in a widespread manner. This is an optional feature and is available only if it has been purchased.

Command Syntax

Important! The maximum length of a message that can be broadcast at one time is **989** characters.

The message is executed at the command line using the **wgui_notify** command. This command can be executed in three different formats:

1. **wgui_notify <"*message* "> <Return>**
   For example:
   wgui_notify "This is an example message from the administrator to the users of the NTP System."
   <Return>
2. **echo <*message* > | wgui_notify <Return>**
   For example:

echo This is an example message from the administrator to the users of the NTP System. | wgui_notify <Return>

3. **wgui_notify <Return>**

   <*message* > <Return>

   <Ctrl> <d>

   For example:

   wgui_notify <Return>

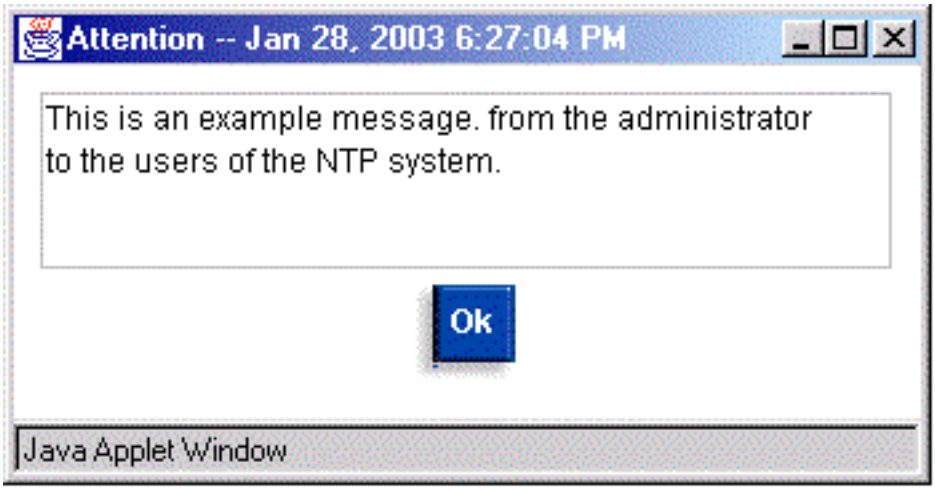
   This is an example message from the administrator to the users of the NTP System.

   <Return>

   <Ctrl> <d>

   Important! After **<Ctrl> <d>** is entered, there may be a slight pause while the message is broadcast and before your system prompt is returned.

After the **wgui_notify** command is executed, a message box (below) is displayed on the BB-GUI user screen.



Install and Uninstall Client Software for the BB-GUI

Overview

Purpose

The client software includes the following components, described below:

- "BB-GUI client software components" (p. 6-60)
- "Pattern Painter software components" (p. 6-61)
- "Adobe Acrobat reader component" (p. 6-61)

Use these procedures for all client software components.

Task	Procedures
Install	"Install Client Software for the BB-GUI" (p. 6-62)
Uninstall	"Uninstall Client Software for the BB-GUI" (p. 6-71)

BB-GUI client software components

You can download the BB-GUI software components from the following web site: **`<machine ip>:4618/ClientInstallation.html`**.

Important! Please note that:

- On all PC platform, if the Java plug-in is ever reinstalled, the provisioning software must be reinstalled also.
- Set your proxies to the hostntp machine. NTP does not recommend using automatic proxies.

To run the BB-GUI, users must have the BB-GUI client software installed on their PCs. This software includes two components:

- Java provisioning component (all platforms)
- Java Jar files

Important! If you try to access any BB-GUI page from a machine without the Java plug-in installed, your browser will automatically be redirected to a client installation page. The Java JRE is not delivered with the BB-GUI client software. Consult your internal IT department for information on how to obtain and install the Java JRE, or visit the official Sun Java website.

The current officially supported versions of Java JRE are:

- Java SE Runtime Environment (JRE) 6 update 20

Pattern Painter software components

Pattern Painter runs in association with the BB-GUI to display graphical depictions of NTP data. To run Pattern Painter, BB-GUI users must have the following software installed on their PCs:

- NTP Advizor components

  Important! Before you start using Pattern Painter, ensure you disable pop-up window blocking in your browser. See "Disabling pop-up blocker warnings for Pattern Painter sortware" (p. 1-8) for more information.

Adobe Acrobat reader component

The *Adobe Acrobat Reader* software is required to read user documentation files provided in .pdf (Portable Document Format), accessible from the BB-GUI. This software is available from the Adobe System, Inc. website (http://www.adobe.com).

Contents

Install Client Software for the BB-GUI

Overview

During initial system installation, your NTP support organization may assist you in configuring PCs of BB-GUI users. But thereafter, when new BB-GUI users join your work group, you must install the client software they need to access the BB-GUI. You can do this either:

- From CD-ROM (see "CD-ROM installation" (p. 6-62))
- From your intranet, (see "Add and Delete BB-GUI Users" (p. 6-33))

CD-ROM installation

A single CD-ROM labeled "WebGUI CLIENT Software" contains all the client software. See "Install and Uninstall Client Software for the BB-GUI" (p. 6-60) for complete information on the installable software.

Web-based installation

For web-based installation of the client software, you download installation files from the following web site: **`<machine ip>:4618/ClientInstallation.html`** and execute them locally on the PC.

Important! If you do not want to support web-based client software installation in the future, you can free up the disk space by removing all files with a .EXE extension in the $SNASDIR/wgui/html directory on the NTP host.

Task overview

Use the following table to select the appropriate procedures to install the client software.

Component	Procedures	Use when...
BB-GUI client software	• "Install BB-GUI client software — PC" (p. 6-64) • "Example" (p. 6-39)	Adding new users and setting up their PCs to run the BB-GUI **Note:** Install the Pattern Painter client software only if a user will need to access Pattern Painter.
Pattern Painter client software	"Install Pattern Painter software — PC" (p. 6-67)	
Adobe Acrobat Reader	"Adobe Acrobat reader component" (p. 6-61)	

Important! You can install the client software in any order, but for web-based installation it is easier to install the BB-GUI client software first. Order of installation matters for components of the BB-GUI client software in some circumstances. See

"Install BB-GUI client software — PC" (p. 6-64).

Install BB-GUI client software — PC

Purpose

Use this procedure to install the BB-GUI client software on a PC from either:

- Your intranet (if your location supports web-based installation). You download installation files from the following web site:
  <machine ip>:4618/ClientInstallation.html
- CD-ROM

This is a standard PC installation procedure that simply requires you to follow prompts and accept the defaults.

Note: To run BB-GUI client software the Java plug-in must be installed on the machine.

Reference: See "BB-GUI client software components" (p. 6-60) for a description of this software.

Notes

- If you install the software while the Java plug-in is active (your browser is running), you MUST reboot your PC. Otherwise you will get a provisioning error when you try to use the BB-GUI. To avoid having to reboot, exit your browser before installing the software (as instructed in the procedure).
- If you reinstall the Java plug-in, you MUST then reinstall the Java provisioning software. You can install "over" the current installation of the Java provisioning software or the plug-in (you do not have to uninstall first).

Check Version

To view the generic and date of the BB-GUI client software currently loaded on the PC, access Settings>Control Panel>Add And Remove Programs. The NTPWebgui Client listing displays the current version and date.

Procedure

Use this procedure to install the BB-GUI client software.

1 If you are installing from:

- Your intranet, close all applications that may be running on the PC EXCEPT your browser, and go to *Step 2*.
- CD-ROM, close any applications that may be running on the PC, INCLUDING all browser windows, and go to *Step 3*.

2 Download the installation file from the following web site: **<machine ip>:4618/ClientInstallation.html**, as follows:

- Put it on your PC desktop, access it from there in the next step, and remove it from the desktop when the installation is complete.
- Point your browser to the Web Based GUI Client Installation Download Page.

  Reference: For how to access the BB-GUI Launch page, see Chapter 3 in the *BB-GUI User's Guide*.

  If the Java plug-in is NOT already installed on your PC, AND you are using the:

  – Mozilla or Firefox browser, you are automatically redirected to the Web Based GUI Client Installation Download Page.

  – Internet Explorer browser, click **Yes** when a window asks if you want to install and run ntp.exe, wait for the installation program to display a welcome window, click **Install Core Web GUI Client**, and go to *Step 4*.

  For Internet Explorer, you may see an error message unless your internet security option for Active-X controls is set to "low" for your local intranet (set through **Tools -> Internet Options... -> Security**). If necessary, consult your network administrator or internet support personnel for assistance in setting the appropriate option.
- Read the instructions for the ntp.exe file, and then left-click the **ntp.exe** link.

  Result: A Save As... window pops up.
- Save the installation file on your PC desktop.

3 If you are installing from:

- Your intranet, run the installation program. To do this, either

  – From the Windows **Start** menu, select **Run** and enter ***Drive:/directory/filename*** (specify the drive, directory, and filename from *Step 2*).

  – Double-click the filename (from *Step 2*) in Windows Explorer.
- CD-ROM:

  – Load the CD labeled "WebGUI CLIENT Software" into the CD-ROM drive.

  Result: The Client CD installation window is displayed.

  If the window does not pop up, select **Start -> Run**, and then enter **Drive:/webgui/windows/ntp.exe** (where **Drive** is your CD-ROM drive).

  – Click **Install Core Web GUI Client**.

  Result: A standard PC installation program starts, and a welcome window is displayed.

4 Click **Next** to accept the default.

Result: A window lists the BB-GUI client software components.

5

- Uncheck option **WEB GUI Provisioning**, if you don't want to install Java provisioning software.
- Check option **Installl Java JAR files** if you want install the Java JAR file on the local machine

6 Click **Next**.

Important! Unless you have information to the contrary from your network administrator, do NOT select the option to install the Java JAR file on the local machine.

Result: A window shows the destination directory for the installed software.

7 Click **Install**.

Result: Progress of the installation is displayed. .

8 Click **Finish**.

Result: If you are installing from:

- Your intranet, you are done. Skip the next step.
- CD-ROM, the original installation window (*Step 3*) is displayed.

9 If you are installing from CD-ROM, select **Exit**, remove the CD from the CD-ROM drive, and store it according to local practice.

END OF STEPS

Install Pattern Painter software — PC

Purpose

Important!

- *Upgrading or Reinstalling.* Before upgrading or reinstalling, be sure you have deleted existing Pattern Painter software (via Control Panel > Add/Remove Software).
- *Web-based installation*. This procedure assumes you have already installed the BB-GUI client software. See "Install BB-GUI client software — PC" (p. 6-64).
- *Reboot*. If you are instructed or prompted to reboot your PC, do so.

Use this procedure to install the Pattern Painter client software on a PC from either: your intranet (if your location supports web-based installation) or CD-ROM. This is a standard PC installation routine that simply requires you to follow the prompts and accept the default selections.

1 If you are installing from:

- Your intranet, close all applications that may be running on the PC EXCEPT your browser, and go to Step 2.
- CD-ROM, close any applications that may be running on the PC, INCLUDING all browser windows, and go to Step 3.

2 Download the installation files, as follows:

- Point your browser to the BB-GUI Launch page (or any BB-GUI page), and then click the **Client Installation** button to go to the Web Based GUI Client Installation Download Page.

  Reference: For how to access the BB-GUI Launch page, see Chapter 3 in the *BB-GUI User's Guide*.

  For Internet Explorer, you may see an error message unless your internet security option for Active-X controls is set to "low" for your local intranet (set through **Tools -> Internet Options... -> Security**). If necessary, consult your network administrator or internet support personnel for assistance in setting the appropriate option.
- Left-click the **ntp_ad.exe** link.

  Result: A Save As... window pops up.
- Save the installation file to a drive on your PC.

3 If you are installing from:

- Your intranet, run the installation program. To do this, either
  - Double-click the filename (from *Step 2*) in Windows Explorer OR from the Windows **Start** menu, select **Run** and enter ***Drive:/directory/filename*** (specify the drive, directory, and filename from *Step 2*).
- CD-ROM:
  - Load the CD labeled "WebGUI CLIENT Software" into the CD-ROM drive.

  Result: The Client CD installation window is displayed. (See "Install BB-GUI client software — PC" (p. 6-64) for an illustration of this window.)

  If the window does not pop up, select **Start -> Run** and enter ***Drive*:/webgui/windows/ntp_ad.exe** (where *Drive* is your CD-ROM drive).

  Result: A standard PC installation program starts, and a welcome window is displayed.

4 Click **Next** to continue.

Result: A window shows the destination directory for the installed software.

5 Click **Next** to accept the default and continue.

Result: A window lists Pattern Painter software components.

6 Select **Pattern Painter** and **Visual Insights**, and click **Next** to continue.

Result: A window indicates that the components you selected will be installed.

7 Click **Next** to continue.

Result: A window prompts you to close any applications that may be running.

8 Click **OK** to continue.

Result: A window with an icon in the upper left is displayed that allows you to change the directory where the software will be installed.

9 Accept the default directory, and then click the icon to continue.

Result: Windows show the progress of Pattern Painter setup, and indicate when setup is complete.

10 Click **OK** to continue.

Result: Windows indicate that the Pattern Painter software is being installed.

11 You may need to do the following. If not, continue with the next step.

- Click **OK** to continue.
  Result: A window is briefly displayed indicating that the Visual Insights installation is beginning, followed by a welcome window for installing the Visual Insights component.
- Click **Next** to continue.
  Result: A window prompts you to select the folder to install the Visual Insights component.
- Accept the default folder, and then click **Next** to continue.
  Result: Windows shows the progress of the installation, and indicate when setup is complete.

12 Click **Finish**.

Result: A window shows that the setup has executed.

13 Click **Finish** to continue.

Result: The original installation window is displayed (*Step 3*).

14 Click **Exit Installation**.

15 If you installed from:

- Your intranet, remove the file you downloaded in *Step 2*.
- CD-ROM, remove the CD from the CD-ROM drive and store it according to local practice.

END OF STEPS

Things to remember

Important! After the ntp_ad.exe program executes on a client PC, you may remove the residual files and folders to save disk space (about 33M). The default location of the files is *C:/Temp*. However, you may have specified a different path during installation. The residual files will exist whether the installation was done via the CD or downloaded from the server.

Important! Before you start using Pattern Painter software, ensure you disable pop-up windows blocking in your browser. See "Disabling pop-up blocker warnings for Pattern Painter sortware" (p. 1-8) for more information.

Uninstall Client Software for the BB-GUI

Task overview

Use the following procedures to uninstall the client software from the PCs of BB-GUI users.

Important! You do NOT have to uninstall the BB-GUI client software or the Pattern Painter client software to install a new version. You can "install over" the older version.

Component	Procedures	Use when...
BB-GUI client software	“Uninstall BB-GUI client software — PC” (p. 6-72)	A BB-GUI user's PC is taken out of service from NTP (to free up disk space. on the PC)
Pattern Painter client software — PC only	“Uninstall Pattern Painter client software — PC” (p. 6-74)	The Pattern Painter client is installed only if a PC user used Pattern Painter for graphical output.

Uninstall BB-GUI client software — PC

Procedure

Use this procedure to remove both components of the BB-GUI client software from PC: Java provisioning software and Java plug-in (see "BB-GUI client software components" (p. 6-60)). Or you can remove (and reinstall) either of these components separately. You can remove these components in any order.

1 From the Windows **Start** menu, select **Settings -> Control Panel -> Add/Remove Programs**.

Result: The Add/Remove Programs Properties window is displayed, with a scrolling list of software.

2 To remove the Java provisioning software:

- Select **NTPWEBGUI Client** from the scrolling list, and click the **Add/Remove** button.
  Result: A standard uninstall program is launched, followed by a welcome window.
- Accept the **Automatic** uninstall option (the default), and click **Next** to continue.
  Result: A standard uninstall window is displayed.
- Click **Finish** to perform the uninstall.
  Result: A message states that the Java provisioning software is being removed from the PC.

  Important! If prompted to remove:
  - Shared components, remove them.
  - Any remaining files that the uninstall utility could not remove, click **Details** to see a list of the files, and delete them from Windows.

3 To remove the Java plug-in:

- Select **Java 2 Runtime Environment Standard Edition** from the scrolling list (*Step 1*), and click the **Add/Remove** button.
  Result: A prompt asks you to confirm the uninstall.
- Click **Yes** to continue.

  Important! If prompted to remove:
  - Shared components, remove them.
  - Any remaining files that the uninstall utility could not remove, click **Details** to see a list of the files, and delete them from Windows.
  - When you see the following message, click **OK** to finish: `Uninstall successfully completed`.

Result: Messages indicate the progress of the uninstall.

END OF STEPS

Uninstall Pattern Painter client software — PC

Purpose

Use this procedure to remove the Pattern Painter software from a client PC. This is a standard Windows uninstall procedure that simply requires you to follow the prompts and accept the default selections. *Reference:* See "Pattern Painter software components" (p. 6-61)).

1 From the Windows **Start** menu, select **Settings -> Control Panel -> Add/Remove Programs**.

Result: The Add/Remove Programs Properties window is displayed, with a scrolling list of software.

2 One at a time, in any order, select the following software from the scrolling list, click the **Add/Remove** button, and follow all prompts and messages:

- ADVIZOR Components `<release_number>`
  If prompted to remove:
- Shared components, remove them.
- Any remaining files that the uninstall utility could not remove, click **Details** to see a list of the files, and delete them from Windows.

END OF STEPS

How Users Access NTP

Purpose

You must inform users how to access the NTP interface(s) for which you have administered them.

Use this reference to inform users how to access NTP. Most users will access NTP through the BB-GUI (or SUI).

Access	Administrator	Analyst
BB-GUI	*URL, Web User ID, and password*. Go to the BB-GUI URL configured when your NTP support organization installed and configured the BB-GUI, and enter your Web User ID and password.	
SUI and system commands	*Host login and password*. Log on the NTP host, to go to the operating system shell that was assigned in "Create a host user ID" (p. 6-10).	Normally analysts do not need shell access.

7 Modify Users

Overview

Purpose

When you add a Network Trouble Patterning software user you set up how the system works for that user (see “Add an NTP user” (p. 6-22)). This chapter tells how you can later modify a user's setup.

Similarly, after you give a user access to the browser-based GUI (BB-GUI), you can later change the initial information you set up (see “Modify BB-GUI User Information” (p. 7-6)).

Contents

Introduction

Overview

Scope

Modifications can affect all users, individual users, or either, for example:

- Individual users — assigning a user to an FDC group
- All users — redefining an FDC group
- Either — assigning a printer, either one user's, or a new default for all users who do not have an individual printer assignment.

Sections in this chapter indicate the scope of procedures.

Special note for RDS

If you have RDS (reference data synchronization) (refsynch), if you modify a user on one host of a host pair, the changes are made on the other host automatically at 00:30 when the **`bdr_syncref`** command runs from crontab. However, if you add or delete a user, you must do so on BOTH systems in the host pair. See Chapter 12, "Reference Database Synchronization (RDS)".

Task overview

This table lists things you can modify for users, and indicates the interface affected.

Just because something appears in this table does not imply you need to administer it. Typically, the initial defaults are used.

Some user attributes, such as permission to switch between FDC groups and network groups, are set SEPARATELY for the BB-GUI. A user can have one assignment for the BB-GUI and a different assignment for the SUI.

Interface	To modify...	Use...	Reference
all	FDC groups, and the FDCs in them	**`dbedit`** on fdcgroup and fdcgroupmap tables	"Create an FDC group" (p. 7-19)
	Network groups and segments, and the entities in them	**`dbedit`** on netgroup, netgroupmap, netseg, and netsegmap tables	"Define Network Groups and Segments" (p. 7-34)

Interface	To modify...	Use...	Reference
unrestricted shell	Access to operating system cron functions	edit cron.allow and cron.deny files	"Create a command group" (p. 7-10)
BB-GUI	BB-GUI user information, including: • user description • password • administrator permission • exception level displays • Ascreen navigation buttons • color of display • font size of display • Max table size • FDC group • network group and segment assignment and permissions	Web User Administration page	"Modify BB-GUI User Information" (p. 7-6)

Interface	To modify...	Use...	Reference
SUI	Command group — assign to a user	**mod_cmdgrp** command	"Change user command group (mod_cmdgrp)" (p. 7-15)
	FDC group — assign, to determine which FDCs appear on output	**mod_fdcgrp** command	"Change user FDC group (mod_fdcgrp)" (p. 7-25)
	FDC group — give a user permission to switch among groups	**dbedit** on fdcpermit table	"Purpose" (p. 7-26)
	Entities — assign a network group or segment to determine which appear on output	**mod_netgrp** command	"Change user network group (mod_netgrp)" (p. 7-44)
	Entities — give a user permission to switch among network groups or segments	**dbedit** on netpermit table	"Change user network group (mod_netgrp)" (p. 7-44)
	Several defaults for all users, (such as printer and output formats) that are set by environment variables.	**admset** command	"Reprocess CDRs" (p. 10-42)

Modify BB-GUI Users

Modify BB-GUI User Information

Purpose

A BB-GUI administrator can use the Web User Administration Page to modify the user information for all BB-GUI user IDs. Any BB-GUI user can modify a subset of this information for his or her own BB-GUI user ID. See "Web User Information Page" (p. 6-46) for a list BB-GUI user information and who has permission to modify it.

Reference: For procedures to add and delete BB-GUI users, see "Add a BB-GUI user" (p. 6-54) and "Delete BB-GUI Users" (p. 6-55).

Procedure

Use this procedure to modify the information displayed on the Web User Information page for a BB-GUI user.

1 Go to the Web User Information page for the user.

Result: See "Go to the Web User Information page" (p. 6-48) for the procedure.

2 Change the information in the fields on the page.

Reference: See "Web User Administration page parts" (p. 6-39) for information about the fields.

3 Click **Submit**.

Result: The system saves your modifications.

END OF STEPS

Manage Command Groups

Overview

Purpose

Command groups determine which commands are available to a SUI user. Once a command group is defined, you can assign users to it. Defining the command groups and assigning users to groups are separate tasks:

- “Create a command group” (p. 7-10)
- “Assign Users to Command Groups” (p. 7-14)

Things to remember

Important! Currently, command groups do NOT apply to the BB-GUI. When you give users web user IDs for the BB-GUI, they can execute all BB-GUI pages. See “Add a BB-GUI user” (p. 6-54).

Example

This example illustrates the process for managing a command group and the user impact:

1. Create a command group called "analyst" containing Ascreen and Trap Data.
2. Assign users to the analyst group. (They cannot assign themselves.)
3. The users can access only Ascreen and Trap Data output.

Command groups

- The default group to which new users are assigned is **`allcmds`**, which enables access to all commands.

  Important! The system is installed with the **`allcmds`** group already defined. You do NOT have to define it.
- Any command in allcmds can also be in one or multiple other command groups.
- If you modify a command group, you affect ALL persons assigned to that group.

Database tables for command groups

You use the following tables to manage command groups.

Table	Purpose
"cos Table" (p. A-44) **Important!** You do NOT **dbedit** this table except for custom configuration (see your NTP support organization.	Lists commands you can group and allow users to access (to see the commands, enter **sui find source=command | more**). Commands in this table are of two basic types: • Commands such as Ascreen and Acresolve can be in a user's command group. • Other commands, such as **dbedit**, can only be entered by typing on the command line or in shell.
"cmdgroup Table" (p. A-40)	Names and describes each command group.
"cmdgroupmap Table" (p. A-41)	Defines which commands are in each group.

Contents

List command groups

Purpose

Here are some **sui** commands you can use to list command groups.

Purpose	Command
List all command groups, with a description of each	**sui find source=cmdgroup | more**
List all command groups, and the commands in each group	**sui find source=cmdgroupmap | more**
List commands in a specific command group	**sui find source=cmdgroupmap se= cmdgroup=<*cmdgroup*> | more**
List command groups a specific command is in	**sui find source=cmdgroupmap se= command=acresolve | more**

Create a command group

Purpose

Important! This procedure does NOT apply for the BB-GUI.

Use this procedure to create a command group. *Reference:* For steps that use **dbedit** , see **dbedit** in Chapter 3, "Reference Data Tables" .

1 Log on the NTP host as **ntp** .

2 Use **sui find** to copy the cmdgroup table into a temporary file (temp).

Example: **sui find source=cmdgroup delim=' ":" ' noheader > temp**

3 Use a text editor (such as **vi**) to add a command group to the temporary file.

- *name field* . Specifies a unique name (up to 10 alphanumeric characters) for a command group.
- *description field* . Describes the command group (up to 50 characters). You cannot leave this field blank, but you can enter - (no description).

Example:

```
Name:Dexcription
allcmds:all commands
analyst:analyst cmd group
admin:admin cmd group
```

4 Use the temporary file to **dbedit** the cmdgroup table.

Example: **dbedit -i -t cmdgroup -f temp -s:**

5 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see "Correct dbedit Errors" (p. 3-27) .

6 Confirm that the change was made by using **sui find** to view cmdgroup table.

Example: To confirm that an FDC group named analyst exists, enter

```
sui find source=cmdgroup    se=name=analyst
```

7 Use **sui find** to copy the cmdgroupmap table into a temporary file (temp).

Example: **sui find source=cmdgroupmap delim=' ":" ' noheader > temp**

8 Use a text editor (such as **vi**) to add a line to the temp file for each command you want in the new command group.

- *cmdgroup field* . Names the cmdgroup (for example, analyst). The command group must have been previously defined in the name field in the cmdgroup table (*Step 3*).
- *command field* . Specifies a command to be mapped to the named command group. The command must have been previously defined in the command table.

  Example: This is an example from the cmdgroupmap table for the analyst command group.

```
Cmdgroup Command
analyst:acresolve
analyst:ascreen
analyst:compute
...
```

9 Use **dbedit** to submit the changes.

Example: **dbedit -u -t cmdgroupmap -f temp -s:**

10 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see “Correct dbedit Errors” (p. 3-27) .

11 Confirm that the change was made by using **sui find** to view cmdgroupmap table.

Example: To see commands in a command group named analyst, enter

```
sui find source=cmdgroupmap se=cmdgroup=analyst
```

END OF STEPS

Redefine a command group

Purpose

To change which commands are mapped to a command group in the cmdgroupmap table, start with *Step 7* in “Create a command group” (p. 7-10).

Important! This procedure does NOT apply for the BB-GUI.

Delete a command group

Purpose

To delete a command group, use **dbedit** with the **-d** option to remove the command group:

- FIRST from the cmdgroupmap table
- THEN from the cmdgroup table.

Use **sui find** to create temporary files for **dbedit**, and to check the changes you make to both tables.If you receive a message ending with: "Errors saved in file...", see “Correct dbedit Errors” (p. 3-27).

Important! This procedure does NOT apply for the BB-GUI.

Assign Users to Command Groups

Purpose

Use the **mod_cmdgrp** command to change a user's command group.

Important! This command does NOT apply for the BB-GUI.

User assignment

- By default, all new users are assigned to the allcmds group, which offers all commands as part of the procedure in "Add an NTP user" (p. 6-22). However, if you use a custom attributes file with the **add_ntpuser** command, the user may be assigned to another group.
- A user can be assigned to only one command group at a time.
- Any number of users can be assigned to the same command group.
- Command group assignment applies to the SUI.
- A user can NOT reassign himself or herself to another group.

mod_cmdgrp command

The **mod_cmdgrp** changes a user's command group assignment.

Syntax

mod_cmdgrp username command_group

Parameter	Description
username	(required) The user's login ID on the NTP host (see "Add a User Login ID on the NTP Host" (p. 6-8)).
command_group	(required) The command group to which the user will be assigned. This must already be defined in the cmdgroup table (see "Manage Command Groups" (p. 7-7)). Please note that you can view the command groups by entering **sui find source=cmdgroup | more**

Example:

This command assigns user johndoe to the analyst command group.

mod_cmdgrp johndoe analyst

This command assigns user johndoe to the allcmds command group.

mod_cmdgrp johndoe allcmds

Change user command group (mod_cmdgrp)

Purpose

Important!

- This procedure does NOT apply for the BB-GUI.
- For the SUI, the cmdgroup field in the sysuser table defines the command group to which a user is assigned. Instead of using this procedure, you can **dbedit** the sysuser table to reassign a user's command group. But NEVER **dbedit** sysuser to add or delete a NTP user.

Use this procedure to assign an existing user to a different command group. Be sure you know the name of the command group you will assign the user. See "List command groups" (p. 7-9)

1 Log on the NTP host as **ntp**.

2 Enter **mod_cmdgrp *username command_group***

where:

- *username* is the user's login ID on the NTP host
- *command_group* is the command group the user is to be assigned

Important! The command_group must exist in the "cmdgroup Table" (p. A-40).

Result: There is no message if **mod_cmdgrp** completes successfully. You see messages, if the user is not defined on the NTP host, if you enter an illegal value for the command group, or if you fail to specify a command group.

Reference: See "Manage FDC Groups" (p. 7-16) for complete information on the command syntax.

3 Check to ensure that the change has been made in the cmdgroup field in the sysuser table for this user by entering

```
sui find source=sysuser | grep username
```

END OF STEPS

Manage FDC Groups

Overview

Purpose

FDC groups determine which FDCs' alert cases appear on NTP output. FDC groups are defined by the procedures in "Create an FDC group" (p. 7-19) in this section.

FDC group definitions apply to all interfaces. However, FDC group assignment and access are administered SEPARATELY for BB-GUI users and users of the SUI.

- For the BB-GUI, see information about the FDC Group field on the Web User Administration and Web User Information pages used in "Web User Information page parts" (p. 6-48)
- Otherwise, see "Assign Users to FDC Groups" (p. 7-23)

Example

This illustrates the process for managing an FDC group and the user impact:

1. Create an FDC group called "trunk", consisting of FDCs related to trunking problems.
2. Trunking analysts assign themselves to the trunk FDC group and use Ascreen or Trapalert with no search criteria.
3. Output shows only alert cases with trunk-related FDCs.

Database tables for FDC groups

You use the following database tables to manage FDC groups.

Table	Purpose
"fdc Table" (p. A-68)	Defines all FDCs. You will NOT dbedit this table in the context of user administration, but you will do so if your system adds FDCs.
"fdcgroup Table" (p. A-72)	Names each FDC group.
"fdcgroupmap Table" (p. A-73)	Tells which FDCs are in each FDC group.
"fdcpermit Table" (p. A-75)	(Does NOT apply for the BB-GUI.) Tells which groups each user is permitted to reassign himself or herself to.

FDC groups

The same FDC can be in multiple FDC groups.

Default

"All". NTP is installed with a default FDC group that is assigned to new users unless you set another group in “Add an NTP user” (p. 6-22). The default is null, which means ALL FDC groups.

User self-assignment for FDC groups

Users can switch between any groups they have permission to access.

Contents

List FDC groups

Purpose

Here are some sui commands you can use to list command groups.

Purpose	Command
List all FDC groups, with a description.	**sui find source=fdcgroup | more**
List all FDC groups, with FDCs in each group.	**sui find source=fdcgroupmap | more**
List the FDCs in an FDC group (such as analyst).	**sui find source=fdcgroupmap se= fdcgroup=analyst | more**
List the FDC groups an FDC (such as 1981) is in.	**sui find source=fdcgroupmap se=fdc= 1981| more**
List FDC groups a user has permission to reassign himself or herself to. (Does not apply for the BB-GUI)	**sui find source=fdcpermit se=sysuser= user | more**
List all users and the FDC groups they have permission to reassign themselves to. Permission for the all group means a user has permission for all groups, even though the groups are not listed by this command. (Does not apply for the BB-GUI)	**sui find source=fdcpermit | more**

Create an FDC group

Purpose

Use this procedure to create an FDC group by using dbedit on the fdcgroup and fdrgroupmap tables. *Reference:* For steps that use **dbedit** , see dbedit in Chapter 3, "Reference Data Tables"

1 Log on the NTP host as **ntp** .

2 Use **sui find** to copy the fdcgroup database into a temporary file (temp). The temporary file name can be any name that you choose.

Example: sui find source=fdcgroup delim=' ":" ' noheader > temp

3 Use a text editor (such as **vi**) to add an FDC group to the temporary file.

- *name field* . Specifies a unique name (up to 10 alphanumeric characters) for an FDC group.
- *description field* . Describes the FDC group (up to 50 characters). You cannot leave this field blank, but you can enter - (no description).

Example:

```
Name:Description
analyst:analyst FDC group
dom:domestic FDC group
int:international FDC group
```

4 Use the temporary file to dbedit the fdcgroup table.

Example: dbedit -u -i -t fdcgroup -f temp -s:

5 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see "Correct dbedit Errors" (p. 3-27) .

6 Confirm that the change was made by using **sui find** to view the fdcgroup table.

Example: To confirm an FDC group named dom exists, enter

```
sui find source=fdcgroup  se=name=dom
```

7 Use a text editor (such as vi) to create a temporary file containing the FDCs that you want to put in your new FDC group.

- *fdcgroup field* . Names the FDC group (for example, dom for domestic). The FDC group must have been previously defined in the name field in the fdcgroup table (Step 3).
- *fdc field* . Specifies an FDC to be mapped to the named FDC group. The FDC must have been previously defined in the fdc table.

For an FDC group called jmstest and three FDCs (vca, nca, 106_p2) your file would look like the example below:

Example:

```
jmstest:vca
jmstest:nca
jmstest:106_p2
```

8 Use **dbedit** to submit the changes.

Example: `dbedit -i -t fdcgroupmap -f temp -s:`

9 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see “Correct dbedit Errors” (p. 3-27) .

10 Confirm that the change was made by using **sui find** to view the fdcgroupmap table.

Example: To see FDCs in an FDC group named domestic, enter

```
sui find source=fdcgroupmap     se=fdcgroup=domestic
```

END OF STEPS

Modify an FDC group

Purpose

You can modify an existing FDC group to:

- Add FDCs to the group
- Delete FDCs from the group

To modify an FDC group, start with Step 7 in "Create an FDC group" (p. 7-19), and change which FDCs are in the fdcgroupmap table.

Delete an FDC group

Purpose

To delete an FDCgroup, use **dbedit** with the **-d** option to remove the FDC group:

- FIRST from the fdcgroupmap table
- THEN from fdcgroup table

Use **sui find** to create temporary files for **dbedit**, and to check the changes you make to both tables. If you receive a message ending with: "Errors saved in file...", see "Correct dbedit Errors" (p. 3-27).

Reference: See "Create an FDC group" (p. 7-19) for examples of the **sui find** and **dbedit** syntax.

Important! Be sure no users are assigned to the group before you attempt to delete it. See "Assign Users to FDC Groups" (p. 7-23) for more information.

Assign Users to FDC Groups

Overview

FDC group assignment and access for users are handled SEPARATELY for the BB-GUI and the SUI. A user can have one FDC group assignment and group access on the BB-GUI and a DIFFERENT FDC group and access on the SUI.

Assigning a new user to an FDC group is part of the procedure in "Add an NTP user" (p. 6-22), using the **`add_ntpuser`** command.

Use the following procedures to reassign an existing user to an FDC group and to administer a user's ability to self-assign to FDC groups:

- BB-GUI
  - See the FDC Group field on the Web User Administration and Web User Information pages used in "Web User Information page parts" (p. 6-48).
- Other
  - Use the **`mod_fdcgrp`** command in "Change user FDC group (mod_fdcgrp)" (p. 7-25) (for users accessing one group only)
  - **`dbedit`** the fdcpermit table in "Assign Users to FDC Groups" (p. 7-23) (for users accessing multiple groups)

User assignment

- The system is installed with a default FDC group that is assigned to new users unless you set another group in "Add an NTP user" (p. 6-22). NTP is installed with this default set to null, which means all FDC groups. However, if you used a custom attributes file to add the user, you may have assigned the user to a specific FDC group.
- Normally, internal analysts (those who work for your company), are assigned to the "all" group and can access all FDC groups.
- A user can be assigned to only one group at a time (including the "all" group), but you can give users permission to switch among groups.
- Any number of users can be assigned to the same group.
- If you modify a group, you affect every user assigned to that group.

User reassignment

You enable users to reassign themselves to FDC groups as follows.

To let a user...	You do this...	Reference
Use only one group.	Assign the user to that group.	"Change user FDC group (mod_fdcgrp)" (p. 7-25)
Reassign self to any group.	Assign the user to all groups (null).	
Reassign himself or herself to some groups.	FIRST assign the user to one group. THEN give the user permission for other groups.	• "Change user FDC group (mod_fdcgrp)" (p. 7-25) • "Purpose" (p. 7-26)

mod_fdcgrp command

The **mod_fdcgrp** command changes a user's FDC group assignment.

Syntax

mod_fdcgrp username fdc_group

Parameter	Description
username	(required) The user's login ID on the NTP host (see "Add a User Login ID on the NTP Host" (p. 6-8)).
fdc_group	(required) The FDC group to which the user will be assigned. This must already be defined in the fdcgroup table (see "Manage FDC Groups" (p. 7-16)), or nothing (null) for all groups. **Default:** Null (blank) — all groups. Please note that the default may be changed for your system. See the FDC_GROUP variable in "Assign or Modify FDC Group and Network Group/Segments for BB-GUI Users" (p. 7-28).

Example:

- This command assigns the user johndoe to the "test" FDC group.
  mod_fdcgrp johndoe test
- This example allows a user to access all groups (the default "null").
  mod_fdcgrp johndoe

Change user FDC group (mod_fdcgrp)

Purpose

Use this procedure to reassign an existing user to:

- ONE FDC group (such as a user external to your company)
- ALL FDC groups

Do NOT use this procedure to change the list of groups a user is permitted to switch among if you assign a specific group (see "Purpose" (p. 7-26))

Procedure

Important!

- This procedure does NOT apply for the BB-GUI.
- For the SUI, the fdcgroup field in the sysuser table defines the FDC group to which a user is assigned. Instead of using this procedure, you can **`dbedit`** the sysuser table to reassign a user's FDC group. But NEVER **`dbedit`** sysuser to add or delete an NTP user.

Be sure you know the name of the FDC group to which you will assign the user. See "List FDC groups" (p. 7-18).

1 Log on the NTP host as **`ntp`**.

2 Enter **`mod_fdcgrp`** *`username fdc_group`*

where:

- *`username`* is the user's login ID on the NTP host
- *`fdc_group`* is the FDC group to which the user is to be assigned.

Result: There is no message **`if mod_fdcgrp`** completes successfully. You see messages if the user is not defined on the NTP host or if you enter an illegal (or no) value for the FDC group,

Reference: See "mod_fdcgrp command" (p. 7-24) for complete information on the command syntax.

3 Verify that the change has been made in the fdcgroup field in the sysuser table for this user by entering **`sui find source=sysuser | grep user`**

END OF STEPS

Give user FDC group permission

Purpose

Use this procedure to add a group to the list of FDC groups a user can switch among. The user must already be created via the **add_ntpuser** command.

Procedure

Important! This procedure does NOT apply for the BB-GUI.

Reference: For steps that use **dbedit**, see **dbedit** in Chapter 3, “Reference Data Tables” .

1 Log on the NTP host as **ntp**.

2 Enter **sui find source=fdcpermit se=sysuser=** *login* where *login* is the login of the user.

Result: Output lists each fdcgroup the user has permission to switch to.

3 Use **sui find** to copy the fdcpermit table into a temporary file (temp).

Example: **sui find source=fdcpermit delim='":"' noheader > temp**

4 Use a text editor (such as **vi**) to edit the temporary file to add or modify a user's FDC group.

- **sysuser field**. Specifies a user's login ID from the sysuser table. A user can have multiple entries, each line with a different fdcgroup.
- **fdcgroup field**. Specifies the fdcgroup the user can reassign to himself or herself to.This group must have been previously defined in the fdcgroup table.

5 Use **dbedit** to submit the changes.

Example: If the changes are in a file named temp, enter
dbedit -u -t fdcpermit -f temp -s:

6 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see “Correct dbedit Errors” (p. 3-27).

7 Confirm that the change was made by using **`sui find`** to view the fdcpermit table.

Example: For user johndoe, enter **`sui find source=fdcpermit se=login=johndoe`**

END OF STEPS

Assign or Modify FDC Group and Network Group/Segments for BB-GUI Users

Purpose

The **mod_wguigrp** command assigns or modifies FDC groups and/or network groups and segments for multiple BB-GUI users in one step.

mod_wguigrp command

Syntax

mod_wguigrp -f | -n [-g <grp1,grp2, ..>] [-w <web_user_id1, web_user_id2>] [-i -u -d -l]

Parameter	Description
-f	(The *-f* or *-n* option is required.) Apply changes to fdcgroups.
-n	(The *-f* or *-n* option is required.) Apply changes to netgroups/segments.
-g	Specify group(s) *<grp1, grp2>*.
-w	Specify web user id(s) *<web_user_id1,web_user_id2>* to be impacted by change. Can also be specified as **all**.
-i	Insert the additional group(s) specified by *-g <grp1,grp2,..>* to current user assignments. As a result, All previous and newly added assignments are shown. If specified group(s) are already assigned for particular user, no action is taken.
-u	Unify (or assign) the group(s) specified by *-g <grp1,grp2,..>* for specified user(s) and discard all previously assigned groups.
-d	Delete fdc group(s) for specified user(s).
-l	List assigned groups for all user available in system.
-c	Synchronizes LDAP data with *Oracle* database: • used with *-f* option, removes all inconsitancies with fdc data. *Example:* **mod_wguigrp -c -f -w all** • used with *-n* option, removes all inconsistencies with net group and segments data *Example:* **mod_wguigrp -c -n -w all**

Examples

This command appends FDC group(s) for specified user(s)

mod_wguigrp -f | -n [-g <grp1,grp2, ..>] [-w <web_user_id1, web_user_id2>] -i

This command unifies FDC group(s) for specified user(s)

mod_wguigrp -f [-g <*grp1,grp2, ..*>] [-w <*web_user_id1, web_user_id2*>] -u

This command deletes FDC group(s) for specified user(s)

mod_wguigrp -f [-g <*grp1,grp2, ..*>] [-w <*web_user_id1, web_user_id2*>] -d

This command lists assigned groups for all user available in system

mod_wguigrp -f | -n -l

Manage Network Groups and Segments

Overview

Purpose

Network groups and segments determine the entities users see on output. For example you might group entities by:

- Entity type or function
- Geographical areas or load areas
- Operations center, for managers to monitor their own entities only or quickly switch to monitoring entities belonging to another center
- A customer's PBXs, to enable customers to monitor their own equipment (and no one else's).

Network groups (and segments) are defined by the procedures in "Define Network Groups and Segments" (p. 7-34).

Network group and segment definitions apply to all interfaces. However, network group and segment assignment and access are administered SEPARATELY for BB-GUI users and users of the SUI.

- For the BB-GUI, see information about the Network Group/Segment field on the Web User Administration and Web User Information pages used in "Web User Information page parts" (p. 6-48)
- Otherwise, see "Assign Users to Network Groups and Segments" (p. 7-42)

Example

This example illustrates the process for managing a network group and the user impact:

1. You create an network group called "dms", consisting of DMS switches.
2. An analyst who monitors DMS switches assigns himself or herself to the dms group and runs Ascreen or Trapalert with no search criteria.
3. Output shows alert cases for DMS switches only.

Database tables

You use the following database tables to manage network groups and segments.

Table	Purpose
"netseg Table" (p. A-112)	Names each network segment.
"netpermit Table" (p. A-110)	Tells which entities are in each network segment.

Table	Purpose
"netgroup Table" (p. A-108)	Names each network group.
"netgroupmap Table" (p. A-109)	Tells which network segments are in each network group.
"netpermit Table" (p. A-110)	(Does NOT apply for the BB-GUI.) Tells which network groups and network segments each user is permitted to reassign himself or herself to.

Network segments and groups

- You can put entities into subgroups called segments, and you can combine segments into groups.
- You can create as many as 300 segments.
- The same entity can be in multiple networks segments AND groups.
- You can create a network group that contains just one network segment (but normally this is not done).

Default

Default group is all, which offers all network groups (and segments).

User self-assignment for network groups

Users can switch between any network groups or segments they have permission to access. See "Change user network group (mod_netgrp)" (p. 7-44).

Audit

To audit network segments, enter audit `-t` netseg (see "Application Audits" (p. 3-49) for how to audit).

TNs override network filtering

TN grouping overrides network filtering.

Example:

An entity in a user's network group has alert case X, whose TN is shared by alert case Y from an entity NOT in the user's network group. Alert case Y is listed on Ascreen output.

To get rid of alert case Y, the user can ungroup it from the TN. More drastically, you can have your NTP support organization disable automatic TN grouping system-wide. If you do that, analysts can still manually group alert cases into TNs.

Contents

List network segments and groups

Purpose

Here are some **sui** commands you can use to list network segments and groups

Purpose	Command
List all groups, with a description.	**sui find source=netgroup | more**
List all groups, with segments in each group	**sui find source= netgroupmap | more**
List segments in a group (example: group ohio).	**sui find source=netgroupmap se=netgroup= ohio | more**
List groups that a segment is in (example: segment columbus).	**sui find source=netgroupmap se=netseg= columbus| more**
List all network segments, with a description	**sui find source=netseg | more**
List all network segments, with CLLI codes in each.	**sui find source= netsegmap | more**
List segments an entity is in (example: CLLI DNVR222222).	**sui find source=netsegmap se=ne= DNVR2222222| more**
List all users and the network segments and groups they have permission to reassign themselves to. (Does not apply for the BB-GUI)	**sui find source=netpermit | more**

Define Network Groups and Segments

Overview

Use these procedures to define network groups and segments:

Create a network segment

Purpose

Use this procedure to create a network segment by modifying the netseg and netsegmap tables. *Reference:* For steps that use **dbedit** , see **dbedit** in Chapter 3, "Reference Data Tables"

1 Log on the NTP host as **ntp** .

2 Use **sui find** to copy the netseg table into a temporary file (temp).

Example: **sui find source=netseg delim='":"' noheader > temp**

3 Use a text editor (such as **vi**) to add a new network segment to the temporary file (temp).

- **name field.** Specifies a network segment (up to 10 characters). Cannot be already used in the netseg or netgroup tables.
- **description field.** Describes the segment (up to 50 characters).

Example:

```
Name:Description
sv0gdins01:107networkstement
sv0gdins02:107networksegment
```

4 Use **dbedit** to submit the change.

Example: **dbedit -u -i -t netseg -f temp -s:**

5 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see "Correct dbedit Errors" (p. 3-27) .

6 Confirm that the change was made by using **sui find** to view the netseg table.

Example: To confirm a network segment named columbus exists, enter
`sui find source=netseg se=name=columbus`

7 Use **`sui find`** to copy the netsegmap database into a temporary file (temp).

Example: **`sui find source=netsegmap delim='":"' noheader > temp`**

8 Use a text editor (such as **`vi`**) to add to the temporary file a line for each entity you want to put in the new network segment.

- **`netseg field.`** Specifies the name of the new network segment. The network segment must have been previously defined in the name field in the netseg table (Step 3).
- **`ne field.`** Specifies the name of an entity to be in the new network segment. The ne must be one of the following:
  - clli defined in swarch
  - scpclli defined in scparch
  - ne in stparch
  - adjcilli in adjarch
  - "?", which represent an unknown entity. The "?" entity can be assigned to network segments so users will see alerts and cfims with a "?" in a network element field. The network segment "all" contains "?" by default.
- **`type field.`** Specifies the type of entity in the ne field. Valid values are:
  - sw
  - stp
  - scp
  - adj
  - "-", which indicates the field is not applicable or there is no data available.

Example:

```
sv0gdins01:sv0gdidm001:sw
sv0gdins01:sv0gdidm002:sw
```

9 Use **`dbedit`** to submit the changes.

Example: **`dbedit -u -i -t netsegmap -f temp -s:`**

10 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see “Correct dbedit Errors” (p. 3-27) .

11 Confirm that the change was made by using **`sui find`** to view the netgroup table.

Example: To see entities in a network segment named columbus, enter
`sui find source=netsegmap se=netgroup=columbus`

END OF STEPS

Create a network group

Purpose

Use this procedure to create a network group by using **dbedit** on the netgroup and netgroup tables.

1 Log on the NTP host as **ntp** .

2 Use **sui find** to copy the netgroup database into a temporary file (temp).

Example: To copy netgroup database into a file named temp, enter
sui find source=netgroup delim='":"' noheader > temp

3 Use a text editor (such as **vi**) to add a line with a new network group to the temporary file.

- **name field.** Specifies a unique name for the network group (up to 10 characters). The name cannot already be used in the netseg or netgroup table.
- **description field.** Describes the network group (up to 50 characters) This field cannot be blank, but you can enter "-" for null.

4 Use **dbedit** to submit the changes.

Example: dbedit -u -i -t netgroup -f temp -s

5 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see “Correct dbedit Errors” (p. 3-27) .

6 Confirm that the change was made by using **sui find** to view the netgroup table.

Example: To confirm an FDC group named ohio exists, enter
`sui find source=netgroup se=name=ohio`

7 Use a text editor (such as **`vi`**) to create a temporary file containing the network segments that you want to put in your new network group.

- **`netgroup`** — Specifies the network group. The network group must already be defined in the netgroup table (Step 3).
- **`netseg`** — Specifies a network segment that will be in the network group. The network segment must have been previously defined in the netseg table (see "Create a network segment" (p. 7-35)).

For a network group called jmstest and three network segments (seg1, seg2, seg3) your file would look like the example below:

Example:

```
jmstest:seg1
    jmstest:seg2
    jmstest:seg3
```

8 Use **`dbedit`** to submit the changes.

Example: `dbedit -i -t netgroupmap -f temp -s:`

If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see "Correct dbedit Errors" (p. 3-27) .

9 Confirm that the change was made by using **`sui find`** to view the netgroupmap table.

Example: To see network segments in a network group named ohio, enter
`sui find source=netgroupmap se=netgroup=ohio`

END OF STEPS

Modify a network group or segment

Overview

To modify a network group or segment to add or delete elements it contains.

- Network segments — start with Step 7 in "Create a network segment" (p. 7-35) and change which CLLIs are in netsegmap.
- Network groups — start with Step 7 in "Create a network group" (p. 7-38) and change which segments are in netgroupmap.

Delete network group or segment

Before you begin

Before deleting a network group or segment, use the BB-GUI Web User Information page (see "Web User Information Page" (p. 6-46)) to reassign any users currently in the group/segment. Unless each user in the impacted network group or segment is reassigned, that user will default to a network group or segment of "all".

> **Important!** Remember to select Submit at the bottom of the Web User Information Page for each user to update the assignment in the system. Additionally, each user should stop/restart their browser session for the update to take effect.

Procedure

To delete a network group or segment, use **`dbedit`** with the **`-d`** option to remove the group or segment from the appropriate tables:

- Network segments — FIRST the netsegmap table and THEN the netseg table
- Network groups — FIRST the netgroupmap table and THEN the netgroup or netseg table

Use **`sui find`** to create temporary files for **`dbedit`**, and to check the changes you make to the tables. If you receive a message ending with: "Errors saved in file...", see "Correct dbedit errors" (p. 3-30).

Hint: See "Create a network segment" (p. 7-35) *and* "Create a network group" (p. 7-38) *for examples of the* **`sui find`** *and* **`dbedit`** *syntax.]*

Assign Users to Network Groups and Segments

Purpose

Network group and segment assignment and access for users are handled SEPARATELY for the BB-GUI and the SUI. A user can have one network group/segment assignment and access on the BB-GUI and a DIFFERENT network group/segment assignment and access on the SUI.

Assigning a new user to a network group or segment is part of the procedure in "Add an NTP user" (p. 6-22), using the **add_ntpuser** command.

Use the following procedures to reassign an existing user to a network group or segment and to administer a user's ability to self-assign to network groups and segments:

- BB-GUI
  - See the Network Group/Segment field on the Web User Administration and Web User Information pages used in "Web User Information page parts" (p. 6-48).
- Other
  - Use the **mod_netgrp** command in "Change user network group (mod_netgrp)" (p. 7-44)
  - **dbedit** the netpermit table in "Change user network group (mod_netgrp)" (p. 7-44).

User assignment

- The system is installed with a default group that is assigned to new users unless you specify another network group or segment in "Add an NTP user" (p. 6-22). NTP is installed with this default set to null, which means all network groups and segments. However, if you used a custom attributes file, you may have assigned the new user to a specific network group or segment.
- A user can be assigned to only one network group or segment at a time.
- Any number of users can be assigned to the same group or segment.
- If you modify a group or segment, you affect ALL persons assigned to that group or segment.

User self- reassignment for network groups

You enable users to reassign themselves to different groups, as follows (in this table, group means either group or segment).

Important! These procedures do NOT apply for the BB-GUI.

To let a user...	You do this...	Reference
Use only one group	Assign the user to that group.	"Change user network group (mod_netgrp)" (p. 7-44)
Self-assign to any group	Assign the user to all groups and segments (null).	
Self-assign to a restricted set of groups	FIRST assign the user to one group. THEN give permission for other groups.	"Change user network group (mod_netgrp)" (p. 7-44)

mod_netgrp command

Syntax

```
mod_netgrp username net_group
```

Parameter	Description
username	(required) The user's login ID on the NTP host (see "Add a User Login ID on the NTP Host" (p. 6-8)).
net_group	(required) The new network group or segment to which the user will be assigned. This group must have been previously defined in the netgroup or netseg table (see "Manage Network Groups and Segments" (p. 7-30)). *Default*: Null (blank) — all groups and segments. Please note that the default may be changed for your system. See the NET_GROUP variable in "Reprocess CDRs" (p. 10-42)

Example:

- This command assigns the user johndoe to the dms network group.
  mod_netgrp johndoe dms
- "Null" assignment lets a user access all network groups and segments.
  mod_netcgrp johndoe

Change user network group (mod_netgrp)

Purpose

Use this procedure to reassign an existing user's network group (or segment). You must decide if the user should be assigned to:

- ONE group or segment (such as a user external to your company)
- ALL groups and segments

Do NOT use this procedure to add a group or segment to the list a user is permitted to switch among. Instead use "Change user network group (mod_netgrp)" (p. 7-44).

Before you begin

Be sure you know the name of the network segment or group to which you will assign the user. See "List network segments and groups" (p. 7-33).

Important! This procedure does NOT apply for the BB-GUI.

Important! For the SUI, the netgroup field in the sysuser table defines the network group or segment to which a user is assigned. Instead of using this procedure, you can **`dbedit`** the sysuser table to reassign a user's network group. But NEVER **`dbedit`** sysuser to add or delete a NTP user.

Procedure

1 Log on the NTP host as **`ntp`**.

2 Enter **`mod_netgrp`** *`username net_group`* where

- *`login`* is the user's login ID on the NTP host
- *`net_group`* is the network group or segment to which the user is to be assigned.

  Reference: See "mod_netgrp command" (p. 7-43) for complete information on the command syntax.

  Result: There is no message if **`mod_netgrp`** completes successfully. You see messages if the user is not defined on the NTP host or if you enter an illegal (or no) value for the network group or segment.

3 Verify that the change has been made in the netgroup field in the sysuser table for this user by entering **`sui find source=sysuser | grep user`**

END OF STEPS

Give user network group or segment permission

Purpose

To add a group or segment to the list a user is permitted to switch among, see "Change user FDC group (mod_fdcgrp)" (p. 7-25) , EXCEPT, in place of the fdcpermit table, use the netpermit table.

Important! This procedure does NOT apply for the BB-GUI.

Netpermit table

- sysuser field. Use this field to specify the user's login ID.
- netseg field. Use this field to specify a network group or segment.
  - A segment must be defined by the name field in the netseg table.
  - A group must be defined by the name field in the netgroup table.

Example: Here is an example of the netpermit table.

```
Sysuser Netseg
ampe sv_newyork
amw sv0gdins01
bcj sv_newyork
drs sv_newhork
```

Reference:

- See the instructions on when to use "Change user network group (mod_netgrp)" (p. 7-44) for how this fits with a related procedure.
- See "User self-assignment for network groups" (p. 7-31) for a discussion of reassignment permissions.

Assign or Modify FDC Group and Network Group/Segments for BB-GUI Users

Purpose

The **mod_wguigrp** command assigns or modifies FDC groups and/or network groups and segments for multiple BB-GUI users in one step.

See "Assign or Modify FDC Group and Network Group/Segments for BB-GUI Users" (p. 7-28) for use of this command.

Manage User Environment Variables

Overview

Purpose

Environment variables determine some attributes for the SUI. Since the system provides defaults for these variables, you may seldom, if ever, need to modify them.

Things to remember

Important! None of the environment variables in this section apply for the BB-GUI. Equivalent BB-GUI attributes are defined SEPARATELY. See "Web User Information Page" (p. 6-46) for more information.

How variables are set

The system proves defaults for environment variables. The **`add_ntpuser`** command uses some of these variables if you do not specify an attribute in the attributes file when you add a new NTP user (see "Add an NTP user" (p. 6-22)).

- You can set environment variables that affect all users with the **`admset`** command —see "admset command" (p. 7-49).
- Each user with shell access can set his or her own login's variables via the **`sui set`** command (see "sui set Command" (p. B-45).

Scope

The NTP administrator can set or modify ALL environment variables for either:

- One user — Via **`add_ntpuser`** (new users) or **`admset`** (existing users)
- All users — Via the **`admset`** command to set a new default, used by all users who do not have an individual value

For a list of things you can modify via the **`admset`** command,"User environment variable list (admset)" (p. 7-50).

Important! Users can modify most of their own variables with the **`sui set`** command (see "User environment variable list (admset)" (p. 7-50)).

Defaults

This table explains the use of user environment variable defaults.

Default	Who can set it
Initial default value	No one. It is installed with the system.

Default	Who can set it
New default value	The **ntp** login, using **admset**. The value you set overrides the initial default.
Individual user value (this is not default)	• The **ntp** login, using **admset** • Any administrative user, using **sui set**

Reference: To see initial defaults, see "User environment variable list (admset)" (p. 7-50) or enter **admset -l** and read the descriptions.

Contents

admset command

Purpose

Use **admset** to set environment variables for either a new default or individual users.

Syntax

```
admset -l
admset [-u user] [variable] [value]
```

Parameter	Description
-l	Lists all variables with descriptions.
u *user*	Specifies login ID for whom the variable values are to be listed, set, or unset back to system default.
none	Sets the system default, to either a new default (if you enter a value, or to the initial system default (if you enter no value).

Important! You must be logged on NTP as ntp to use the **admset** command.

List and set user variables

This table shows all the ways you can use **admset**.

Purpose		Enter...
List	All environment variables with definitions (including initial default value (see "User environment variable list (admset)" (p. 7-50). for output).	**admset -l**
	All new defaults (lists only environment variables not using initial defaults).	**admset**
	One user's individual variables (lists the user's environment variables not using initial or new default)	**admset -u *user***
Set	A variable from initial default to a new default	**admset *VARIABLE value***
	One user's variable	**admset -** **u djd *VARIABLE value***

Purpose		Enter...
Unset	A variable from new default back to initial default	**admset *VARIABLE***
	A user's variable back to default	**admset -udjd *VARIABLE***

User environment variable list (admset)

These are the user environment variables you can set from **admset**. You see a list of these variables if you enter **admset -l** (but **admset -l** may list other variables that do not affect your system). Variables that can also be modified with the **sui set** command are noted.

Note that:

- "Format" in this table means choosing which fields to display, and field order (but Compute output has other format considerations).
- For BB-GUI colors, see "Web User Information Page" (p. 6-46).
- Some variables affect only legacy interfaces still used by some customers. Unless otherwise indicated, variables apply to the SUI.

Variable	Function	Values	Modify with sui set?
ACASE_FORM	Format, Find Alert Cases output.	Values: A valid Format. Default: list of Acase fields.	no
ALERT_FORM	Format, Find Alert output.	Values: A valid Format. Default: list of Alert fields.	no
ASCREEN_ FORM	Format, Ascreen output.	Values: A valid Format. Default: list of Acase fields.	no
ASCREEN_ SORT	Sort order, Ascreen output.	Value: a valid Sort list. Default: lda time: **d,lcnt:d**	no
ASCREEN_ SRCHFIELDS	List of fields in the BB-GUI's Ascreen search window.	Default: list of Acase fields.	
CFIM_FORM	Format, Find CFIM.	Values: A valid Format. Default: list of Cfim fields.	no
CFIMTRAP_ FORM	Format, Trap Data output.	Values: A valid Format. Default: list of Cfim fields.	no

Variable	Function	Values	Modify with sui set?
COMP_ECHO	Format, Compute output. Values echoed in the Compute title.	Values: **none** or **all** (default); or a list of one or more of **min, interval**, or **sort**.	yes
FDC_SEARCH	• If "group" — searches without an Fdc are filtered by FDC_GROUP. • If "all" — searches are not filtered.	Default: all	
FDCCOUNT_ FORM	Format, Find on FdcCount tables.	Values: A valid Format. Default: list of FdcCount fields	
FIND_SRCHFIELDS_ ACASE	List of fields in the BB-GUI Find search window for Alert Cases tables.	Default: list of Acase fields.	
FIND_SRCHFIELDS_ ALERTS	List of fields in the BB-GUI Find search window for Alert tables.	Default: list of Alert fields.	
FIND_SRCHFIELDS_ CFIM	List of fields in the BB-GUI Find search window for CFIM tables.	Default: list of CFIM fields.	
FIND_SRCHFIELDS_ LINK	The list of fields in the BB-GUI Find search window for Linkalert tables.	Default: list of Linkalert fields.	
FIND_TIME	Find time. Default time duration for Find on surveillance tables.	Range: a number 1 to 120. Default: 10.	yes
LINK_FORM	Format, Find Linkalert output screen	Values: A valid Format. Default: list of Linkalert fields.	no
MAXSAVE	Finds, default maximum number of user files to save	Range: A number 1 to MAXSAVE_MAX. Default:10000.	no
MAXSAVE_ MAX	Finds, maximum value a user can give for Find's maxsave parameter or the MAXSAVE variable.	Range: A number 1-999999. Default: 100000.	yes

Variable	Function	Values	Modify with sui set?
MAX_GRAPH	The maximum number of distinct x-values for Compute graphs in the GUI. This should be a number between 1 and 100.	Default: 25.	
MIN_COUNT	The minimum value of data points output by Compute. • If OUTPUT is "count" — this should be a whole number between 0 and MAXSAVE minus one. • If OUTPUT is "percent" — this should be a floating-point number between 0.00 and 99.99.	Default: 0.	
NET_SEARCH	• If "group" — searches without a Network Entity are filtered by NET_GROUP. • If "all" — searches are not filtered.	Default: "all".	
NUM_AUTO_ COLS	Format, Compute output. Number of column values used by Compute when the user does not give any.	Range: a number 1 to 12. Default: 7.	yes
OTR_FORM	The output format for Find on OTR tables.	Values: A valid Format. Default: list of OTR fields.	
OUTPUT	Format, Compute output. **Note:** Changing OUTPUT changes MIN_COUNT and MAX_COUNT for the same user, if set. Because the system default for OUTPUT affects the way all MIN_COUNT and MAX_COUNT user defaults are interpreted, we recommend you use the system default.	Values: **`count`** (default) — Compute output is shown by count, and MIN_COUNT and MAX_COUNT are in interpreted as counts; **`percent`** — compute output is shown by percent, and MIN_COUNT and MAX_COUNT are interpreted as percentages.	

Variable	Function	Values	Modify with sui set?
PROC_SIZE	Maximum size to which any user interface process can grow (in bytes).	Range: any positive number. Default: 60000000 (60 Mbytes). Can be overridden with the environment variable NTP_PROC_SIZE.	no
RANGE	Range of rows output by the Find. Syntax when setting a range is:'"30001 - 50000"'For example: **sui admset** **variable=RANGE** **value='"30001 -** **50000"'**	Value: a range *MM-NN* where *MM* and *NN* are both less than MAXSAVE, and the *MM-NN* includes at most 30000 rows. Default: 1-10000.	yes
TRAPALERT_ SRCHFIELDS	List of fields in the BB-GUI Trapalert search window.	Default: all Trapalert fields.	
TRAPCFIM_ SRCHFIELDS	The list of fields in the GUI Trap Data search window. This should be a list of Cfim fields.	Default: all Cfim fields.	
TRAPALERT_ FORM	Format, Trapalert output.	Values: A valid Format. Default: list of Trapalert fields.	no

Manage User Files and Databases

Overview

Purpose

Users can create and save ASCII files and SQL database files. Since, enough of these can accumulate to degrade system performance, so you must ensure unneeded files are deleted. Accumulated databases are potentially more of a problem than accumulated ASCII files. This section explains how user ASCII files and user databases are created, how to recognize when they are a problem for your system, and provides procedures to remove them.

Things to remember

Important! Any user with shell access (SUI users) can create ASCII files in a variety of ways as well as user files with the -w user_file option to **`sui find`** (see your NTP support organization for more information.)

Definition

Database files referred to here are NOT working sets. A working set is automatically created by the system when a user does a find and has s a "ws" in its name. Each one is automatically overwritten by a later find, which prevents them from multiplying. If you remove a working set, however, it causes no harm, since it is replaced by the next find. Although they are called "user files", user-created SQL databases are NOT files (you CANNOT list them with shell commands such as ls or lsc).

How users create and remove ASCII files

Users can remove ASCII files they create only if they have access to the operating system shell. If they do not, you must remove unneeded ASCII files for them.

How users create and remove databases (user files)

- Creation. User databases are created in two ways:
  - Automatically. Each time the user does a Find. The name includes the letters "ws" (for working set).
  - Manually. For example, when a user of the legacy X-GUI selects File > Save to User File on a Find output window. The name is whatever the user called it.

  Automatically created databases do NOT need to be removed, as each is overwritten with a later find.

Manually created databases must eventually be removed, by the user, or by you if the user forgets to remove them.

- Removal. Users without shell access can remove their own manually created databases through the interface they used to create them:

Task overview

Use the information in the following sections to remove user databases and ASCII files if users cannot do so for themselves.

- "Remove User ASCII Files" (p. 7-56)
- "Remove User Databases" (p. 7-57)

Contents

Remove User ASCII Files

Purpose

Use this procedure whenever disk resources run low and users have accumulated unneeded ASCII files.

1 Log on the NTP host as root.

Important! To remove another person's files, you must log on as **`root`**.

2 Go to the user's home directory, and enter *file* *

Result: All files in the user's home directory are listed, each identified as ASCII or other type file.

3 Are there too many ASCII files in the user's home directory?

- If NO, never mind. Done.
- If YES, go to the next step.

Important! "Too many" depends on your system resources.

4 Does the user have access to shell on the NTP host?

- If YES, ask the user to use the operating system **`rm`** command to remove unneeded files from his or her home directory, including ASCII files saved from the GUI.
- If NO, coordinate with the user, and then log on as **`root, cd`** to the user's home directory and use the operating system **`rm`** command to remove the files yourself,

END OF STEPS

Remove User Databases

When to use

Remove user databases when periodic checks show an accumulation of databases or when the master error log indicates a space problem.

You use the **sui remove** command to remove user databases (see "sui remove Command" (p. B-42)).

> **Important!** Each automatically created database has a *ws* in its name. These you do not need to remove, since each is overwritten by later finds, which prevents them from multiplying. However, if you DO remove one, it will cause no harm, since it will be replaced by subsequent finds.

Max # extents message

"Max # extents" messages in the master error log indicates you are running out of space, possibly due to an accumulation of user-created databases (or possibly due to other problems not discussed here — see *Oracle* references).

You use the **ptspace** command to check extents for your system see "ptspace Command" (p. 7-59)).

Example

This is an example of a "max # extents" message in the master error log:

```
ERR001 CHRON_OBJECTS insert failed: error code -1631, ORA-

01631: max # extents (500) reached in table

DB$.CHRON_OBJECTS;
```

Reference: For how to monitor the master error log, see "master Log" (p. 10-25) .

Periodic checks

You use the **ptspace** command to do periodic checks (see "ptspace Command" (p. 7-59)). You can also use the **sui list** command "sui list Command" (p. B-40)).

Remove user databases

Purpose

Use this procedure to check the space used for user databases and to remove them if necessary.

1 Log on the NTP host as **ntp**.

2 Run the **ptspace** command to check user databases.

Example: ptspace usr

For a different view of a user's databases, log on NTP as that user and run the **sui list** command. See<xref linkend="id-34032_00Dsuicmd"/> for more information.

Reference: See "ptspace Command" (p. 7-59) for more information.

3 Use the sui **remove** command to remove unneeded databases.

Example: Example: To delete database files mary1 and mary2, belonging to login mtm, (not your current login) enter

```
sui remove force files=mtm/mary1,mtm/mary2
```

Reference: See "sui remove Command" (p. B-42) for more information.

END OF STEPS

ptspace Command

Purpose

The **ptspace** command lists user databases for all users, or for users you name. It is useful to check if users have accumulated too many databases.This command is a script provided by NTP. It is not found in *Oracle* references. You must be logged on as ntp to run **ptspace**.

When to use

Use **ptspace** as follows:

- Periodic checks. Typically, an accumulation of user database is a rare problem. Checking every few months is normally sufficient.
- "max # extents" message. A "max # of extents" in the master error log may be causes by too many user databases (see "Max # extents message" (p. 7-57)).

ptspace and sui remove

After you have run **ptspace**, you can use the "sui remove Command" (p. B-42) to remove unneeded user files.

Syntax

```
ptspace tablespace [username]
```

Parameter	Description
tablespace	(required) Any SQL database tablespace (to check user databases, use **user**).
username	(optional) Any user ID, to list only one user's databases. This parameter makes sense only if you **put user** in the first parameter

Example:

- To check all user databases for all users, enter **ptspace** usr
- For other purposes, you can look at any tablespace, especially:
  - **ptspace** reference — lists reference databases
  - **ptspace** system — lists *Oracle* internal databases

Output

Output is a list of user-created databases. Output has the following fields:

Field	Function
OWNER	User who created the database.

Field	Function
SEGMENT_NAME	Database name.
PART	
TS	
BLKS	How many blocks are in the database.
EXTENTS	Number of extents the database is divided among.

Output example

This is an example of an output from the command **`ptspace usr`**

```
OWNER  SEGMENT_NAME  PART  TS   BLKS  EXTENTS
-----  ------------  ----  ---  ----  -------
VID    TESTSUI             USR  3456  42

DB     USERTABLE           USR  8     1
```

Too many extents

To see the total number of extents for your system, you must use **`ptspace`** with each tablespace in turn, and sum the number of extents for all. However, if you see too many extents for the user tablespace alone, you already know you need to delete some user databases. The following table gives guidance:

This total number of extents	Means
1-20	No problem
20-50	Acceptable
50-200	System performance is affected. If you approach 200, take action.
200-500	Take action immediately
500	Danger of system failure

Restrict User cron Functions

Overview

Purpose

You can assign restricted cron functions to users on a per-user basis.

Scope

Typically, only users with administrative access to NTP (shell access) will need cron functionality.

Background

If any functions using crontab are to be restricted to a set of users, those users must be listed in the */usr/lib/cron/cron*.allow file. This file contains a list of the logins that have cron access, one name on each line.

If instead of cron.allow,an empty cron.deny file exists in /usr/lib/cron, user access to cron functions is unrestricted.

Important! Cron.allow and cron.deny must have permissions set (**`chmod`**) to 644.

Contents

Restrict user cron access

Purpose

Do the following, as appropriate:

- To restrict user access to cron functions, add them to the cron.allow file.
- To allow unrestricted user access to cron functions, remove the cron.allow file entirely and create an empty cron.deny file in the same directory.

Reference:

- For complete information on cron functions, see crontab in the reference documentation for your operating system.
- For managing NTP (not user) cron function, see Chapter 2, “Start and Stop”.

8 Threshold Administration

Overview

Purpose

Network Trouble Patterning software monitors a set CFIM fields known as an Alert Type. This process is known as *thresholding*. Measurements exceeding preset thresholds warn of abnormal conditions or *alerts*.

Contents

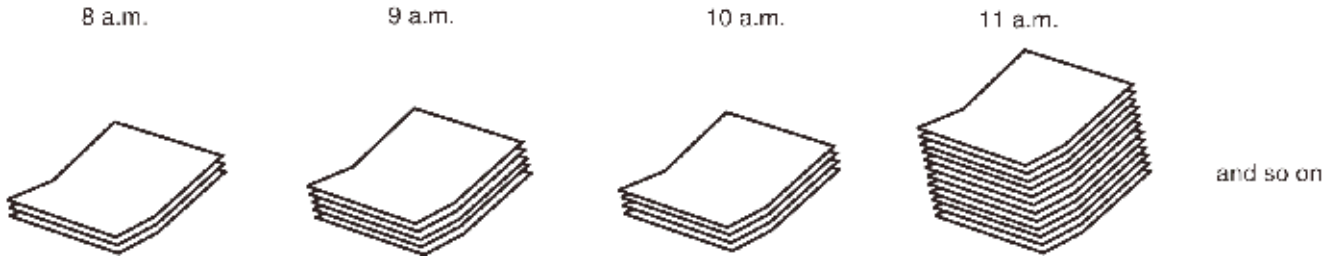
Thresholding

Overview

Purpose

Threshold example

This is a simplified view of thresholding.



- Imagine each CFIM arriving on a separate sheet of paper. Each hour, you collect all CFIMs from (for example) one RE (that is, one network element) and put those CFIMs into a separate pile. You might see, for example, a short pile for 8 a.m., a tall pile for 11 a.m., and so on.
- Do this every day for two weeks, and then figure out the average pile height for each hour of the week. Each hour's average is its threshold.
- Then, if a pile grows higher than its threshold, you know the RE has encountered something unusual.

CFIMs to Alert cases

When a "pile" of CFIM's crosses a threshold, it becomes an alert case, and:

1. When a threshold is crossed, we take the "pile" of CFIMs, summarize it into an "alert case", and put it (as one line) on Alert Case output.
2. Each time the alert case is again above threshold, we add the new over-threshold pile of CFIM's to the same alert case.
3. If an alert case stays below threshold for 4 hours (2 hours if CFIM count is low), we take the alert case off Alert Case output.

Manual thresholds

You may have millions of thresholds, so we automatically create and update them for you. However, you can have your system administrators manually override specific thresholds.

User-Defined Alerting

NTP has a basic set of alert types pre-defined.

With the optional User Defined Alerting feature, NTP can threshold on ANY set of CFIM fields (or a single CFIM field), as long as it doesn't conflict with default alerting, or exceed capacity limits.

Additional alert types may be added by contacting Lucent Customer Support.

FQ versus Alert Type

It is possible for you to threshold on (to alert on) any set of CFIM field types. Such a set is called an alert type.

Each alert type must be purchased separately, and may require customization of your system.

Thresholding can potentially threshold on any CFIM field value or set of field values. This set of fields is called an FQ (fundamental quantity). The default FQ is the RE field alone, used for the Call Volume Alerts.

To clarify:

- "nycmny03t20/nea" is an FQ (a specific re and a specific fdc).
- "re/fdc" is an alert type (a field type and another field type).

Consultants can be contracted to create additional FQs for any set of CFIM fields. Such FQs are not documented in this book.

Examples of some custom alert types that have been created are as follows:

- fdc/ccd — Country code alerting FQ
- fdc/ccd/rt — Country route alerting FQ

Default Alert Types

The default alert types are:

- FDC
- RE or DE
- LSP — The week is divided into LSPs (traditionally, 48 LSPs).

For each alert types, there are two sets of thresholds for two types of intervals:

- *5-minute*. Detects bursty problems.
- *Hourly*. Detects chronic problems.

Example: With 400 FDCs, 20 REs, 200 DEs, two intervals (5-minute and hourly), and 48 LSPs, you would have up to 8,448,000 thresholds.

Additional types of thresholding

In addition to 5-minute and hourly thresholding, NTP provides:

Retroactive alerting. Allows alerting for previous hours, and for the receipt of records in batches, allowing all of them to be evaluated for the hour in which they occurred.

System day alerting. Takes all thresholds for FDCs you pick and thresholds on them daily. This is most appropriate with operator trouble report (OTR) type CFIMs or other types of low-volume alerting.

Enhanced mass call alerting. Automatically used to put mass call alerts on the Alert Cases and Trap Alerts screens. Supports segmentation between different network groups. Each group can only see data originated or derived from their own set of REs. See "Enhanced Mass Call Alerting" in the *BB-GUI User's Guide*.

Contents

Alert Case Outputs

Threshold outputs

Thresholding creates alert cases, seen on these outputs:

- "Alert Cases Page" in the *BB-GUI User's Guide*. Shows open alert cases only. Updates every 5 minutes.
- "Trap Alerts Page" in the *BB-GUI User's Guide*. Shows only the first alert (5-minute interval) in an alert case. Most alert case fields are omitted. Updates in real time.
- "Find Page" in the *BB-GUI User's Guide*. Shows both open and closed alert cases. No updating.

Note

- *Alerts table*. In addition, the “alert_levels” (p. A-15) shows tallies for each interval in an alert case.
- *Alerts*. Technically (in error and help messages), an "alert" is one interval in an alert case.

Introduction to alert cases

About alert cases:

- *CFIM summary*. An alert case is a one-line summary on or more cfims, possibly hundreds, even thousands, of CFIMs.
- *Modify*. You can modify alert cases, for example, to close, comment, or assign them. These modifications are seen by all users. See "How to modify an alert case (overview)" (5-8) in the *BB-GUI User's Guide*.
- *Mass Call Alerts*. Shows mass call events shown as alert cases.
- *Map an Alert Case to its CFIMs*. NTP allows a user to "drill down" to the CFIMs associated with an Alert Case.

Setting Up Alerting Configuration Tables

Creating New Alerts

User Defined Alert Types is a optional feature. If you have purchased this feature you can create a new alert type. To create a new alert type:

- Edit the alertdef table to add a new alert type.
- Edit the alertperiod table to define the alerting period.
- Edit the alertfq table to define FQ columns for the alert.
- Edit the alert_levels table to define the alert levels (if desired).
- Validate the alert.
- Activate the alert.

These steps are explained in more detail in the sections that follow.

Editing Tables

Use the following procedure to edit the alertdef, alertperiod, and alertfq tables for a new alert type.

1 Update the alertdef table with the modifications.

Result: To update or insert a record for the alertdef table, enter (where *name* is the fieldname that will be analyzed)

```
sui find source=alertdef search=type=re noheader delim = '"|"' > temp
```

The file resembles this:

```
#Type|Script|Srcmodel|Threshtype|Src_hist|Tmpl_tab|Lspgran|Me
   ancalc|Weightfac|Low_pct|High_pct|Low_cap|High_cap|Sensitiv
   ity|Datecol|Max_latency|Quorum|Filter
   re|fdc|cfim|high|cfim_p|pptempmap_fdc|5|binom|.05|.0001|.99
   99|.01|.99|1|-|-|80|-
   de|fdc|cfim|high|cfim_p|pptempmap_fdc|5|binom|.05|.0001|.99
   99|.01|.99|1|-|-|80|-
```

- Use a text editor (such as vi) to change the line to define the record you want to update or insert, and then save the file.
- To insert or update the record from the temp file into the alertdef table, enter **`dbedit -ui-f temp -t alertdef -s '|'`**
- If you receive a message ending with:
  - "dbedit completed successfully".
  - "Errors saved in file...", see “Correct dbedit Errors” (p. 3-27) .

Reference: Use the **describe** command for information on what to put in each field of the table. Also see "alertdef Table" (p. A-18) .

2 Update the alertperiods table with the modifications.

- To update or insert a record for the alertperiods table, enter (where *name* is the fieldname that will be analyzed)

  sui find source=alertperiods search=fieldname=*name* noheader delim = '"|"' > temp

- Example output of find might look like:

```
#Type|Period|At|Savecnt|Cntfreq|Alfreq|Acfreq|Reset|Tolerance
     |Min_thresh|Closecai1|Closecai2|Closecnt
   re|1|1m|n|1|0|0|n|1|1|24|48|50
   re|5|5m|n|1|1|5|n|1|4|24|48|50
   re|60|1h|n|60|60|60|n|1|4|2|4|50
   re|1440|1d|n|5|5|5|y|60|4|2|4|50
   de|1|1m|n|1|0|0|n|1|1|24|48|50
   de|5|5m|n|1|1|5|n|1|4|24|48|50
   de|60|1h|n|60|60|60|n|1|4|2|4|50
   de|1440|1d|n|5|5|5|y|60|4|2|4|50
```

- Use a text editor (such as *vi*) to change the line to define the record you want to update or insert, and then save the file.
- To insert or update the record from the temp file into the alertperiods table, enter **dbedit -ui-f temp -t alertperiods -s '|'**
- If you receive a message ending with:
  - "dbedit completed successfully".
  - "Errors saved in file...", see "Correct dbedit Errors" (p. 3-27) .

  Reference: Use the **describe** command for information on what to put in each field of the alertperiods table. Also see "adjarch Table" (p. A-13) .

3 Update the alertfq table with the modifications.

- To update or insert a record for the alertfq table, enter (where *name* is the fieldname that will be analyzed)

  sui find source=alertfq search=fieldname=*name* noheader delim = '"|"' > temp

- Example output of find might look like:

```
sui find so=alertfq se=type=re noh delim='"|"'
#Type|Fieldname|Archtable|Archfield|Tmpl_key|Data_sourcere
re|re|db$.swarch|clli|n|y
re|fdc|db$.fdc|fdc|y|n
```

- Use a text editor (such as *vi*) to change the line to define the record you want to update or insert, and then save the file.
- To insert or update the record from the temp file into the alertfq table, enter
  dbedit -ui-f temp -t alertfq -s '|'
- If you receive a message ending with:
  - "dbedit completed successfully".
  - "Errors saved in file...", see "Correct dbedit Errors" (p. 3-27) .

  Reference: Use the **describe** command for information on what to put in each field of alertfq table. Also see "alertfq Table" (p. A-19) .

4 If desired, update the alert_levels table with the modifications. The alert_levels table is used to specify behavior of the AL (Alert Level) field in the alert and acase records.

- To update or insert a record for the alert_levels table, enter (where *name* is the fieldname that will be analyzed)
  sui find source=alert_levels search=fieldname=*name* noheader delim = '"|"' > temp
- Example output of find might look like:

```
sui find so=alert_levels se=alert_type=re noh delim='"|"'
#Alert_type|Al|Min_sev
re|ma|5
de|ma|5
```

- Use a text editor (such as *vi*) to change the line to define the record you want to update or insert, and then save the file.
- To insert or update the record from the temp file into the alert_levels table, enter
  dbedit -ui-f temp -t alert_levels -s '|'
- If you receive a message ending with:
  - "dbedit completed successfully".
  - "Errors saved in file...", see "Correct dbedit Errors" (p. 3-27) .

Reference: Use the **`describe`** command for information on what to put in each field of alert_levels table. Also see “alert_levels” (p. A-15) .

END OF STEPS

Validating, Activating, and Disabling Alert Types

After a New Alert is Created

After a new alert type is created using the alertdef, alertperiod, and alertfq tables, the alert is in the "created" state.

> **Important!** In order to create or delete "alert types", you must have the optional feature "User Defined Flexible Alerts" enabled.

To make the new alert active, login as "ntp" and:

- Validate the alert with the **fa_validate** command
- Activate the alert with the **fa_activate** command

If it becomes necessary to stop or modify the alert, use the **fa_disable** command.

fa_validate Command

The **fa_validate** command looks at the configuration tables and verfies that the alert you've added is syntactically correct. It also looks at how many FQs might be generated for the alert(s) and verifies that the system has the capacity to handle it.

fa_validate [alert=<*alerttype*>]

Where *<alerttype>* is the name of the new alert. If you do not specify an alerttype, the system defaults to all newly created types.

fa_activate Command

The **fa_activate** command creates applicable tables (mean and threshold) and starts alerting immediately after restart of the system. To use this command, Oracle must be running, and NTP must be stopped.

fa_activate [alert=<*alerttype*>]

Where *<alerttype>* is the name of the new alert. If you do not specify an alerttype, the system defaults to all newly created types.

fa_disable Command

The **fa_disable** command stops the alert and moves the associated tables to an inactive state and changes the status of the alert back to created.

fa_disable alert=<*alerttype*>

For this command, an alerttype must be specified. The alert will remain disabled until **fa_validate** and **fa_activate** are run again.

Managing Thresholding

Thresholding tables

Thresholds are managed in two sets of tables (where xx is an alert type, such as cc):

- **mean_xx** — Where NTP accumulates counts used to automatically create thresholds, and where you can dbedit to affect soaks and LSP updates.

Example:

```
sui find so=mean_re se=lspid=b11 and fdc=vca noh delim='"|"'
#Lspid|Accum|Frozen|Count_mean|Re|Fdc
b11|84|-|.345959|clmbohxeds0|vca
```

- **man_thresh_xx** — Where you can dbedit to define manual thresholds.

Example:

```
sui find so=mean_re se=lspid=b11 and fdc=vca noh delim='"|"'
#At|Modified|Lspid|Thr|Thr_type|Min|Max|Re|Fdc
5m|03/08/27 10:56|-|-|h|4|-|-|-
```

Reference: These tables are discussed in more detail in the remainder of this chapter.

Switching Threshold Calculation Speed

Purpose

You can switch the threshold calculation convergence speed between three settings: freeze, rapid and normal. This might be used in a case where the behavior of the network has recently changed, to allow computed thresholds to catch up more quickly.

Use the **thresh_adjust** command to switch the speed:

thresh_adjust [alert=<*alert_type*>] <*adjust value*>

Where:

- Alert is the alert type. The default is all alert types.
- Adjust value is
  - freeze (0.0)
  - rapid (0.25)
  - normal (0.1)

Change automatic alert case closing

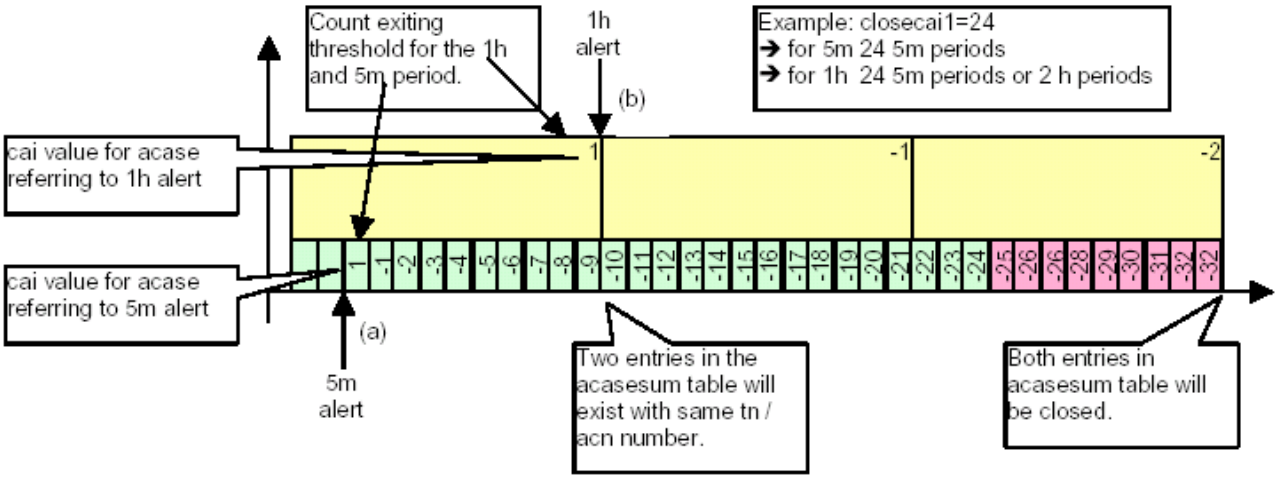
Purpose

When an alert case stops crossing thresholds for enough consecutive intervals, it automatically closes. A closed alert case disappears from Ascreen Output but stays in the acase table — with "closed" in its Status field until the next 5-minute update.

Automatic alert case closing is controlled by CLOSECAI1, CLOSECAI2, and CLOSECNT in the alertperiods table. These values represent the number of alert periods of inactivity that must elapse to close the alert case. For example, 24=24 hours. CLOSECNT is used to differentiate between high and low count alert cases. If COUNT is less than CLOSECNT, CLOSECAI1 is used. Otherwise, it uses CLOSECAI2.

Clarification of display of 5m and 1h alert intervals

This section explains the behavior of an alert case that has active alerts for both 5 minute (5m) and 1 hour (1h) alert intervals, and refers to the following illustration:



- An alert (for a certain FQ) will automatically close when it stops crossing threshold for CLOSECAI1/CLSECAI2 consecutive intervals for that alert type.

The alert screen shows a negative increasing CAI value until the number of consecutive intervals is reached for that FQ.

  – For the 5min alert types: CAI counts until - CLOSECAIX.
  – For the 1h alert types: CAI counts until - CLOSECAIX / 12.

- A specific FQ can have alerts active for both 5m and 1h alert types. This is based on the alertperiods table.
  – If an FQ crossed the 5m threshold value on a 5m boundary, an alert case is opened for a 5m alert type in the acasesum table.
  – If an FQ crossed the 1h threshold on the hour boundary, an alert case is opened for a 1h alert type in the acasesum table.
- There is only one entry in the acase table at a time and there are two entries in the acasesum table. The acase view table is presented, which is a combination of the acase and acasesum tables. Therefore, you see a 1h alert at the hour boundary if it crossed the 1h threshold.

  If an FQ crosses a 1h threshold and, at the next 5m boundary, the same FQ does not cross the 5m threshold, you will still see the 1h alert case on that 5m boundary.
- Therefore, an FQ can be both a 1h and 5m open alert case at the same time. When there is a 1h open alert case for a FQ, the 5m alert case for that FQ remains open - even through the CAI value for the 5m alert case is less than the value for CLOSECAI2.

  The 1h keeps the 5m alert case open, allowing the 5m CAI value to get progressively more negative.
- Consecutive alerts for the same FQ, but with different alert intervals, have the same tn and acn number and refer to the same alert case.
- By default, on the Alert Cases Page we see one line per alert case (the one that last crossed the threshold). In the illustration (above):
  1. The 5m alert will be displayed *(a)*, at a 5m boundary,
  2. After the 1h alert occurs *(b)* at the 1h boundary, the latest alarm is displayed. This is because at the hour boundary the 1h threshold for that FQ exceed the 1h threshold value for that LSP. The 1h alert type is displayed instead. The same is true for a 5m boundary.
- The Alert Case page (or **`sui ascreen`** command) shows the most recent alert cases. If both a 5m and 1hr alert are active for an alert case at the same time, the 5m alert takes precedence and is always shown, except on the hour boundary when the hourly alert is shown.

Dynamic Alert Level based on FDC and Lcnt

Purpose

When the NTP alerting system generates an alert case (acase), an initial severity is assigned to the acase based on the severity of the underlying alerts. Generally, this severity remains static throughout the life of the acase.

The Dynamic Alert Level based on FDC and Lcnt feature can change the severity assigned to an acase. The feature also allows the severity to change during the life of the acase. The user can specify an FDC, count, and a severity in the fdc_sev table. If an acase is generated for that FDC and the lcnt field of that acase exceeds the count specified by the user in the fdc_sev table, then the severity is set to the severity specified by the user. This allows a user to designate certain failures as more serious and to focus remediation efforts more effectively. At every 5-minute alert interval, the acase is again checked against the fdc_sev table. If the lcnt field no longer exceeds the count field specified in the fdc_sev table, the severity of the acase will be changed to the normal severity of the underlying alerts.

Reference: See the “fdc_sev Table” (p. A-70) table in Appendix A for information on how the table works.

Feature Activation

The Dynamic Alert Level based on FDC and Lcnt feature is optional. The option is called “ROPT_FDCSEV”. The falert process will not process the contents of the fdc_sev table unless this option is enabled. Please contact Alcatel-Lucent personnel to enable this feature.

Specifying Severity

Use the following steps to specify a count and a severity in the fdc_sev table for a particular FDC.

1 Log on the 8920 NTP host as ntp (you must be logged on as ntp to proceed).

2 Enter

```
sui find so=fdc delim='"|"' > ./filename
```

to save the names of all FDCs in the file (where **filename** is the name you choose for the file containing all FDCs).

3 Use a text editor (such as vi) to look through all FDCs saved in the file (enter **vi filename**), and then choose the FDC for which you want to specify a new severity.

4 Enter

sui find so=acase se=fdc=FDCname format=al, lcnt delim='"|"'

to display the current entries of the **al** and **lcnt** fields in an **acase** for the chosen FDC, where:

- **FDCname** - is the name of the chosen FDC.
- **al** - indicates the alert level of the chosen FDC. Valid values for this field are: "cr" -critical, "ma" - major, "mi" - minor.
- **lcnt** – indicates the last alert CFIM count (lcnt) is the count of CFIMs for the last alert record.

5 Use a text editor (such as vi) in order to save in a file the min_count and severity values for the chosen FDC. The file will be used to update the fdc_sev table.

Enter

vi .fdc_sev.db

and update the file with the following: severity, min_count, and FDC (must be a value in the fdc table), and save the file.

```
sevetity|min_count|FDCname
```

6 To insert or update the record from the .fdc_sev.db into the fdc_sev table, enter

dbedit –iu –f ./fdc_sev.db –s '|'

Result: If an acase is generated for the chosen FDC and the lcnt field of that acase exceeds the count specified by the user in the fdc_sev table, then the severity is set to the severity specified by the user.

LSPs

Purpose

Generally, you would NOT want the same thresholds at all times, since traffic levels vary from hour to hour. So, NTP divides the week into LSPs (load set periods) and gives each LSP its own set of thresholds.

This section explains how LSPs are defined.You may never want to change how LSPs are defined, but this information is useful for understanding soaks.

Scope

LSPs are time periods. They cycle weekly. They are defined system-wide. You can NOT have different LSPs for different switches, FDCs, FQs, or logins.

Default LSPs

There are 48 initial default LSPs, as follows:

- 24 LSPs: b0 to b23, hourly, repeated Monday through Friday.
- 24 LSPs: w0 to w23, hourly, repeated Saturday and Sunday:

We show this in the following table (0000 is midnight):

	Business days				Weekend days			
lspid	**b0**	**b1**	**etc.**	**b23**	**w0**	**w1**	**etc.**	**w23**
Time	0000-0100	0100-0200	...	2300-0000	0000-0100	0100-0200	...	2300-0000

View the current LSP

Overview

To see the current LSP, enter **`fa_lsp`** .

The output does NOT show the current hour, which is the first plus second columns of the lsphours table (for example, b1). Instead, this shows what LSP is assigned to the current hour, which is the first plus last columns of the lsphours table (for example, b1).

(If you are using the initial system defaults, the second and last columns hold the SAME values, so current hour [e.g. b1] is the same as current lsp [e.g. b1].)

Example:

You enter **`fa_lsp`** on monday at 12:30 a.m. You might see:

- b0 — From lsphours table, if you use initial default values.
- b1 — From lsphours table, if you set up lsphours to be the traditional 15 LSPs.
- w0 — From the lspcalendar table, on Labor Day, if you set up Labor Day to use weekend (w) LSPs.

Tables where LSPs are managed

Lspdays and Lsphours tables define LSPs and tell where they are used, and the Lspcalendar table overrides where they are used. Here is what you might see if you "sui find" these tables.

Table	sui find example	Output example

lspdays
(See "lspdays Table" (p. A-94) .)
	`sui find source=lspdays noh`
	to see which days of the week are b (business), w (weekend), or other types you may create.
	b and w are initial default types. You can have up to seven types. The more types, the more LSPs to soak.
		`#Day Day`
		`mon b`
		`tue b`
		`wed b`
		`thu b`
		`fri b`
		`sat w`
		`sun w`

Table	sui find example	Output example

lsphours
(See "lsphours Table" (p. A-96) .)
	sui find source=lsphours noh
	to see how many LSPs are defined.
	The first field must be each lspdays type in the lsphours table, the second must be 0-23 (hours) with each lspdays. The third field can be whatever you want. Each unique pair of values in the first and last fields defines a different LSP.
		`#Day Ho Lspid`
		`b 0 0`
		`b 1 1`
		`b 2 2`
		`b 3 3`
		(and so on, up to "b 23 23")
		`w 0 0`
		`w 1 1`
		`w 2 2`
		`w 3 3`
		(and so on, up to "w 23 23")

lspcalendar
See lspcalendar reference table.)
	sui find source=lspcalendar noh
	to see which days of the year are exceptions. For example, you might want Labor Day to use weekend LSPs so it will use weekend thresholds.
		`#YYYYMMDD Datype Description`
		`20000704 W Use weekend LSPs`
		`20001225 W Use weekend LSPs`

Table	sui find example	Output example

lspdaytypes
(See "lspdaytypes Table" (p. A-95) .)
	sui find source=lspdaytypes noh
	Used to define set of daytypes in use and assign default soak period to each. Must be populated here before a new daytype can be used elsewhere.
	Please note that the lspdaytypes table "soak" field controls the length of the soak period. If this value is decreased, thresholds for any FQs that have a soak in progress may become erroneous.
	Therefore, anytime the soak field value is decreased, the **set_resoak** command should be used to resoak any entities that have a soak in progress. See "Re-soak" (p. 8-27) .
		`#Daytype Soak`
		`b 120`
		`w 48`

Tables where LSPs are used

"Tables where LSPs are managed" (p. 8-19) explains that you get a unique LSP for each unique pair of values from the first and last fields of the lsphours table (b0, b1 b2...w0, 21 w2, etc.). Two tables (mean_xx and man_thresh_xx, where xx is an FQ type) use these pairs of values in their lspid fields.

Table	Sui find example	Output example
mean_xx (See "mean_xx Tables" (p. A-102) .)	**sui find source=mean_ccd search=ccd=670** to see what thresholds exist, and their soak status, for each lspid where ccd is 670. There is a unique threshold soaked for each unique set of values for key fields in each mean_xx table. For example, in the mean_ccd table, there is a threshold for each Lspid/Ccd. This output example shows: • A threshold soaked for each weekday (b0 to b23) LSP. • No thresholds yet for weekends (w, or w to w23). Apparently no weekend has been encountered since the new fdc/ccd was detected. • Accum is used to track long_term statistical effects. It will keep growing, even after soak.	Lspid Accum F Count_mean Ccd b17 120 - 1 670 b18 120 - 3 670 b19 120 - 3 670 b20 120 - 3 670 b21 120 - 3 670 b22 120 - 3 670 b23 120 - 3 670 b0 120 - 3 670 b1 120 - 3 670 b2 120 - 3 670 b3 120 - 3 670 b4 120 - 3 670 b5 120 - 3 670 b6 120 - 3 670 b7 120 - 3 670 b8 120 - 3 670 b9 120 - 3 670 b10 120 - 3 670 b11 120 - 3 670 b12 120 - 3 670 b13 120 - 3 670 b14 120 - 3 670 b15 120 - 3 670 b16 120 - 3 670
man_thresh_xx (See "man_thresh_xx Tables" (p. A-98) .)	**sui find source=man_thresh_re** to see if If any manual thresholds have been added for any Lspid's. Use man_thresh_xx where xx is an FQ, such as rt or cc.	#At|Modified|Lspid|Thr|Thr_type|Min|Max|Re|Fdc 5m|03/08/27 10:56|-|-|h|4|-|-|- If Nothing appears, which means none have been added.

LSP threshold adjustment

NTP adjusts thresholds at the end of each LSP.

NTP generates alerts during soak. However,

- *during soak* , all counts collected during the soak period are weighted equally, regardless of alert activity
- *after soak* , new counts are weighted at a fixed % versus the old mean, and counts with associated alerts are discounted.

Refresh thresholds for an LSP

If you have changed means in the "mean_xx Tables" (p. A-102) and do not wish to wait until the end of the LSP for the thresholds to be generated, you can refresh thresholds for the specified lsp(s) by using the following command:

```
lsp_update -T -l <lspid>
```

where lspid is the lspid in the proper format (b1, b2, etc.) or all.

Freeze LSP threshold adjustment

Purpose

NTP adjusts thresholds at the end of each LSP. To freeze or unfreeze a threshold's adjustment, use “Shorten a soak in progress” (p. 8-29), but in Step 6, edit the frozen field, assigning either:

- "y" to freeze
- "-" to unfreeze

Limit LSP threshold adjustment

Purpose

NTP adjusts thresholds at the end of each LSP. To set maximum, minimum, or both, or to limit how far the thresholds can be automatically adjusted, use the following:

- Put "-" in the thr field to suppress alerting on the specified FQ, or all FQs matching wildcards (~).
- Populate the max field, min field, or both.

  Important! *Precedence.* What if, while using this procedures, you add records to a man_thresh_xx table, and those records have overlapping key fields? (Key fields are lspid plus fq.) For what takes precedence see “man_thresh_xx Tables” (p. A-98).

Soaks

Purpose of soaks

To "soak" means to monitor a network to find normal CFIM rates, in order to set NTP thresholds. NTP does soaks in two cases:

- *Initial.* Initial full soak of the entire network when the application is first turned on.
- *New.* After the initial soak, NTP may be triggered to do new, partial, soaks, as explained next.

What a soak does

When a soak is triggered, NTP does the following:

- In a mean_xx table, adds records with each the new (never soaked) value in a key field (a different record for each lspid). (Key fields are lspid plus FQ.)
- In each record's count field, accumulates a weighted average CFIM count for (by default) 120 5-minute periods for each LSP.
- After (default) 120 5-minute periods, uses the count value to generate different thresholds for each lspid, for each alert interval type (at). These thresholds can be seen on the Thresholds display (see “Viewing Thresholds” (p. 8-31)).

Example of new soak

- You add a new FDC of 777000 to your FDC table.
- The first CFIM arrives with new FDC 777000, and with re of clmbohexds0.
- The FQ type named "re" has key fields of fdc and re (see “mean_xx Tables” (p. A-102)). So NTP automatically soaks 777000/clmboheds0, for all LSPs.
- To see these soaks, look in the mean_cc table or on the Thresholds display (see “Viewing Thresholds” (p. 8-31)). For example, enter:

  `sui find source=mean_cc search=re=clmbohexds0`

  Output might resemble the example at “” (p. 8-22).

  Important! *Dashes don't count*. NO soak is done for "-". For example, if a CFIM arrives with a new FDC of 777000, but the CFIM's re and de fields are "-", then no new soak occurs in mean_cc. Also, if an FQ is assigned a manual threshold of "-", that FQ is ignored. Also, a threshold will not be established in the "thresholds" table, until the system has gone through one full "lspid" interval, where default minimum is one day(24 hours).

Re-soak

Purpose

The **set_resoak** command causes a requested set of FQs to begin a resoak. To re-soak, use the following command:

set_resoak alert=<*alert_type*> [*FQname*=<*FQvalue*>[<,*FQvalue*>]]

Where:

- FQname is a valid FQ member
- FQvalue is a valid value for that FQ member

Multiple values for a single member are or'd together. Multiple members are and'd together.

Example:

The command:

set_resoak alert=re re=clmbohexds0 fdc=1,2,3

will resoak all cc FQs where the ccd is one of clmbohexds0 and the fdc is one of 1, 2, or 3.

The system responds with the number of means that will be affected. Enter y to continue with the resoak operation.

How long a soak takes

By default, a soak is for 120 5-minute periods. Since the 120 5-minute periods refer to an LSP, these normally happen 1 hour each day. Each LSP soaks independently. 120 5-minute periods is the equivalent of 2 full weeks.

Shorten all future soaks for an FQ

Purpose

You may want to shorten ALL new soaks for a set of LSPs, affecting all future thresholds that may be created (as they are added to the mean_xx table). Do this by editing the "soak" field in the lspdaytypes table.

Important! It is unwise to soak less than 2 days (24 5-minute periods, as serious inaccuracy could result.

Shorten a soak in progress

Purpose

Use this procedure to shorten an FQ's soaks in-progress (soaks already in the mean_xx table, and whose accum column has not reached maximum — 120 by default).

1 Find the key fields for the FQ's mean_xx table.

Reference: See the "mean_xx Tables" (p. A-102) . Key fields are lspid plus fq.

Example: Key field for mean_cc are lspid, fdc, and re.

2 Use **sui find** with one or more key field values to pull from the mean_xx table all records you want to modify—in order to modify soaks.

Important! Do not update records for the current or previous LSP or you may create a conflict within the system.

Example: Key fields for mean_ccd are lspid, fdc, and ccd. To pull from mean_ccd all records with FDC of XYZ (for all lspid's and ccd's), enter

```
sui find source=mean_cc search=clmbohexds0 noheader delim='
"|" ' > temp
```

3 Use a text editor (such as vi) in the temp file to change values in accum fields to bigger numbers, to shorten soaks; or to the maximum number of soak periods to end the soak. Default maximum is 120, but can vary by FQ (if you had your customer engineer change it). Example of: "sui find so=mean_cc noh m=1 delim='"'|'"'is:

```
#Lspid|Accum|F|Count_mean|Re|fdc
b14|84|-|.345959|clmbohexds0|vca
```

4 Use **dbedit** to replace existing records in the mean_xx file with your changed records.

Example: `dbedit -u -t mean_ccd -f temp -s "|"`

5 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see "Correct dbedit Errors" (p. 3-27) .

6 Remove the temp file.

END OF STEPS

Viewing Thresholds

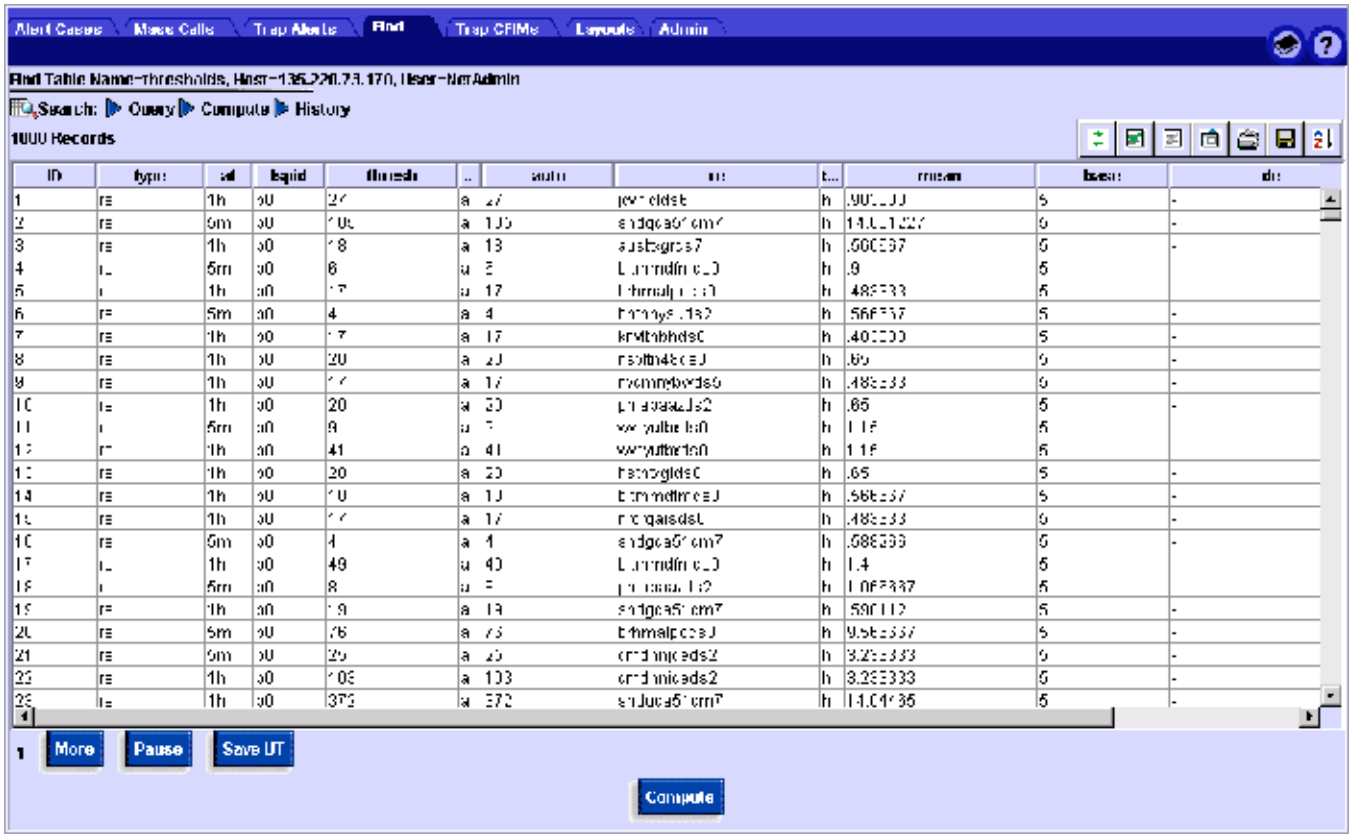
Where to see thresholds

You can see:

- *Manual thresholds* — In the man_thresh_xx table.
- *Thresholds* — in two ways:
  - the command **`sui find so=thresholds`**
  - the THRESHOLDS display (read-only) gives manual, auto, and soak status for all FQ types.

    Access the Thresholds display (shown below) from the BB-GUI using Find > Query > Thresholds.

    Performance of the thresholds display can be slow if a very large amount of data is being selected. To avoid this, use a search expression to limit the data being viewed.



The fields provided in this display are:

Field	Description
type	The alert type (re,de,etc).
at	The threshold interval (5m, 1h, etc).
lspid	The identifier of the load set period associated with this threshold dat(b0,b1,etc.)
thresh	The current threshold in use by the system for this FQ and period.
source	The source of the CURRENT threshold. Values can be: • a - automatic threshold • m - a specific manual threshold • < - a minimum threshold • > - a maximum threshold • x - alerting is manually suppressed.
auto	The current automatic threshold value. Should be the same as CURRENT if no manual or max/min override is in effect.
Thr_type	Type of threshold - High (traditional) or Low.
mean	The current mean value from which the auto threshold was calculated.
base	Base time period to which the mean is normalized.
soaked	The percent of the designated soak that is completed.
RE	The reporting entity that generated the CIM.
DE	The distant entity that the reporting entity was attempting to communicate with.

Manually Adjust Thresholds

Purpose

You can trust NTP to automatically create and adjust thresholds. But if you want, you can manually adjust thresholds in three ways.

To do this	See
Limit how far a threshold can automatically adjust	"Limit LSP threshold adjustment" (p. 8-25)
Turn off thresholds	"Turn off thresholds" (p. 8-34)
Set manual threshold to override automatically created thresholds	"Viewing Thresholds" (p. 8-31)

Notes:

1. *Man_thresh_xx.* The three procedures above all add records to man_thresh_xx tables.
2. *Precedence.* What if, while using procedures above, you add records to a man_thresh_xx table, and those records overlap (affect some of the same thresholds)? For precedence see "man_thresh_xx Tables" (p. A-98).

Minimum Thresholds

The "min" field in the man_thresh_xx tables is important because:

- it establishes a minimum boundary for automatic thresholds. For example, if min=5, and the system computes automatic threshold as 4, the min value will override the automatic threshold value.
- it provides a value to be used when no automatic threshold has been set, such as when the system encounters a new FQ. For example, If min=5 and the wildcard is set to any field, then the system generates an alert and will not set a mean.

Default settings for the system are a wildcard for each alert type with a minimum threshold of 3.

Effectiveness of changes to man_thresh_xx tables

Changes to man_thresh_xx tables don't take effect until the **`lsp_update`** command is run for the LSP affected (see "Refresh thresholds for an LSP" (p. 8-23)). If the lsp_update command is not run, changes are not put in place until after the next end of that LSP, and won't be used until the second subsequent LSP instance.

Turn off thresholds

Purpose

Use “Viewing Thresholds” (p. 8-31) to put "-" in all three of these fields: thr, max, and min.

Important!

- From “man_thresh_xx Tables” (p. A-98), you learn that man_thresh_xx tables use "~" for wildcard in key fields. But thr, max, and min are NOT key fields, so here "~" does not mean wildcard, but means "null".
- If you wish to see alerts immediately, for FQs that are new or so infrequent that they are not tracked normally, wildcard min thresholds must be in place.
- The AI indicator must be set to "on" in swarch and fdc tables for the FQ to alert.

Assign manual thresholds

Purpose

Use this procedure to assign manual thresholds to replace automatically created thresholds.

1 For the FQ whose thresholds you want to manually set, find the key fields for the man_thresh_xx table (where xx is the FQ, such as man_thresh_cc).

Reference: See the "man_thresh_xx Tables" (p. A-98). Key fields are: at, lspid and fq.

Example: Key fields for man_thresh_cc are: at, lspid, fdc, and ccd.

2 Where xx is an FQ, enter

```
sui find source=man_thresh_xx noheader delim='";"' > temp
```

Example: `sui find source=man_thresh_re noheader delim='";"' > temp`

3 Use a text editor (such as *vi*) to open and look at the temp file. If the file holds:

- Nothing, there are no existing manual threshold to modify or to use as templates for new manual thresholds. You must create from scratch a record for each manual threshold you want to add. To see what fields are in each record, see "man_thresh_xx Tables" (p. A-98), or use the **`describe`** command.
- One or more records, there are existing manual thresholds. With these records, you can modify non-key fields to change existing manual thresholds, or modify key fields, to add new manual thresholds.

4 Edit the file as desired, and save the file.

5 Use **`dbedit`** to put your new or changed records into the man_thresh_xx file.

Example: `dbedit -iu -t man_thresh_re -f temp -s ";"`

6 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see "Correct dbedit Errors" (p. 3-27).

7 Remove the temp file.

END OF STEPS

Stop or Restart Thresholding for Entity or FDC via Ai

Purpose

To stop all 5-minute or hourly thresholding on an entity or FDC, but still collect its CIMs and CFIMs, change the FDC's or entity's Ai field to off in the fdc, swarch or other "arch" table. To restart, change the field back to "on".

Scope

Editing an Ai field (in the fdc, swarch or other "arch" table affects ALL thresholds for an entity or FDC.

You can virtually stop just one threshold (one CLLI/FDC/entity-role/5-minute-or-hourly/LSP) or a set of thresholds by using the “man_thresh_xx Tables” (p. A-98) .

Result

If you change an entity's or FDC's Ai field to **`off`** , you remove all thresholds for the entity or FDC from the threshold matrix. This means CIMs and CFIMs are still collected for the entity or FDC, but for the entity or FDC there will be NO:

- Automatic or manual thresholding
- Alert cases where the entity is in the Ne field (or FDC in the Fdc field).
- Automatic threshold adjustments

When to use

Use the following procedure for an FDC or entity that.

- No longer exists. (In this case, also remove the entity. See Chapter 4, “Add Network Elements”).
- Exists, but you do not want to threshold it, or you currently can not threshold on it.

Procedure

Use this procedure to stop or restart all thresholding for an entity or FDC by editing the Ai (alert indicator).

1 If you are starting thresholding, review the information in “Soaks” (p. 8-26) .

2 Log on the NTP host as **`ntp`** .

3 Select the table where you will change Ai (alert indicator) to "off" (for stop) or "on" (for restart).

Reference: Tables are fdc, swarch, and other "arch" tables.

4 Run **find** on the table and send output to a temporary file.

Example:

- For the fdc table, enter
  sui find source=fdc noheader delim='";"' > temp
- For the swarch table, enter
  sui find source=swarch noheader delim='";"' > temp

Result: The table is copied into the temp file.

5 Use a text editor (such as *vi*) to open the file and edit the appropriate line(s) to turn thresholding on or off in the Ai field. Then save the file.

Important! Change no more than 100 lines. If more lines need to be changed, repeat this procedure for each 100.

Example: (This is an example from the swarch table showing clli sv0prf5es01. The Ai field shows thresholding in "on".

```
#Clli;Dpc;Eqtype;Stp;Owner;Hnpa;Ai;Ccd;IPaddress;
```

```
Descriptionsv0prf5es01;-;5ess;sva1;svtst;212;on;-;-;-
```

6 Run **dbedit** with the update option and the temp file for input.

Example:

- For fdc, enter **dbedit -ui -t fdc -f temp -s";"**
- For swarch, enter **dbedit -ui -t swarch -f temp -s";"**

7 Correct errors as you are informed of them by **dbedit** .

8 Remove the temp file.

9 If you started thresholding, make a note of the FDC or entity you are soaking and mark your calendar to check to ensure alert cases are being created for the FDC or entity. If you are using default (10 LSP) soak periods, check in:

- 2 weeks for weekday LSPs
- 5 weeks for weekend LSPs

END OF STEPS

Trunk Busy Notification Feature

Purpose

The optional Trunk Busy Notification feature monitors specific trunk groups for blocking or congestion failures and provides the data about failures to an external application.

Overview

The feature performs the following functions:

- checks specific trunk groups on particular switches for **allbsy** Trouble Category (TC) and when the called digits matches on an entry defined in the 8920 NTP database, at 1 min. intervals,
- induces a single Reporting Entity (RE) to alarm when the number of **allbsy** TC on this RE exceeds the threshold in a 1-min. interval,
- sends the details on each encountered alert to a remote Oracle database.

Additional Alert Type

The feature provides an additional alert type to the existing Alert Cases and Trap Alerts screen outputs. The additional alert type is tagged "**atb**" (all trunks busy).

The following details characterize the functionality of the "**atb**" alert:

- The "**atb**" alert type uses a manually settable threshold that indicates how many **allbsy** failures are permitted in a single minute for a specific RE before an alert is generated.
  Example: Setting the threshold value to 2 indicates that 2 failures in a minute will generate an alert, but a single failure will not. The threshold set to 1 makes every **allbsy** failure generate an alert.
- The "**atb**" alert uses filtering on **TC**, **DIGITS**, and **RE** values provided by the customer.
- The "**atb**" alert supports all normal user interface functions of the Alert Cases and Trap Alerts screens, including support of searching and saving searches, and drill down to individual CFIMs via Find or Pattern Painter.

Trunk Busy Notification Tables

The following reference tables are associated with the Trunk Busy Notification feature:

- "atb_alerts Table" (p. A-22)
- "atb_digits Table" (p. A-23)
- "atb_entities Table" (p. A-24)
- "atb_log Table" (p. A-25)
- "atb_troubles Table" (p. A-26)

Alert Notification

8920 NTP sends a notification to a pre-defined recipient when the "**atb**" alert is received and remote database connection fails. Note that the alert is sent only the first time 8920 NTP cannot access the remote system.

Reference: See "Alert notification" (p. 10-7) for detailed information about setting alert notification.

ATB Alert on Alert Cases and Trap Alerts Screens

8920 NTP lists alert cases on Alert Cases page, the worst at the top. The "**atb**" alerts are updated onto the Alert Cases screen only every 5 min. in order to avoid excessive redraw of that screen.

If you want to see new alert cases as they are generated (in real time) use Trap Alerts. Appearance of **atb** alerts on the Trap Alerts screen occurs on a 1-min. interval.

Retroactive Alerting

Overview

Introduction

NTP alerts on 5-minute and hourly intervals, and expects that records will be received in near real time. Based on this expectation, calls are counted and matched against a threshold every period for the previous period. If records older than the current period are received, they are not counted for alerting purposes. While this works well if the data is received in near real time, it does not work as well for records received in infrequent batches. Retroactive alerting allows alerting for previous periods, and for the receipt of records in batches, allowing all of them to be evaluated for the period in which they occurred.

Setting up Retroactive Alerting

Use the alertdef table to set the max_latency time period to the most late you would expect the data to be. The default is 6 hours. See “alertdef Table” (p. A-18).

Notes

In the alertdef table, set the max_latency table field to the maximum number of minutes that receipt of data might trail the creation of the record by the network element. It must be less than 23 hours (1380 minutes).

> **Important!** The larger this value is set, the more system resources (particularly memory) will be consumed, so set it with diligence, and no not use an unnecessarily large value.

Generation of alerts may then be delayed by that many minutes in cases where incoming data is batched or delayed

Retroactive alerting is not needed for real-time CIM interfaces and associated alerting.

System Day Thresholding

Overview

Purpose

System day thresholds are daily thresholds. They are useful for problems whose CFIMs trickle in so slowly that even hourly thresholds may miss them. If you have this optional feature, you can enable this type of thresholding by configuring the alertperiods table.

Things to remember

Important! If the SDALERT option is not enabled, rows in the alertperiods table referring to daily periods will be ignored.

Compare to normal thresholding

Let us compare normal 5-minute-and-hourly thresholding with system day thresholding.

This type thresholding	Works this way...	Example
Normal 5-minute, hourly, and daily	NTP creates a unique 5-minute, hourly, and daily threshold for each unique combination of FDC, network element (a CLLI), entity role (either reporting or distant), and LSP.	For FDC 1984, if you have ten switches, you have up to 2,880 thresholds, as follows: One FDC X 10 switches X 2 entity roles X 48 LSPs X 3 types of threshold (5-minute, hourly, or daily) = 2,880
System day	The system automatically creates a "1d" threshold based on a 24-hour observation period, but only in those cases where the automatic 5-minute threshold for that FQ is below the system minimum.	If you set FDC 1984 to a system day thresholding, that threshold replaces all 2,880 normal thresholds explained in the example above. Please note that daily thresholds can be assigned default or manual values like any other threshold period.

More differences

Normally, system day alerts behave slightly differently than 5-minute or 1 hour alerts in that when a 1d (1 day) count exceeds it's threshold, it will generate an alert at the next 5-minute period boundary. If the failures continue, it will alert again when another number (specified in <threshold value>) of CIMs have been collected.

For example, if the 1d threshold is 20, you get an alert at 20, 40, 60, etc., until midnight, when the counter is reset.

Contents

Set System Day Tolerance

Background

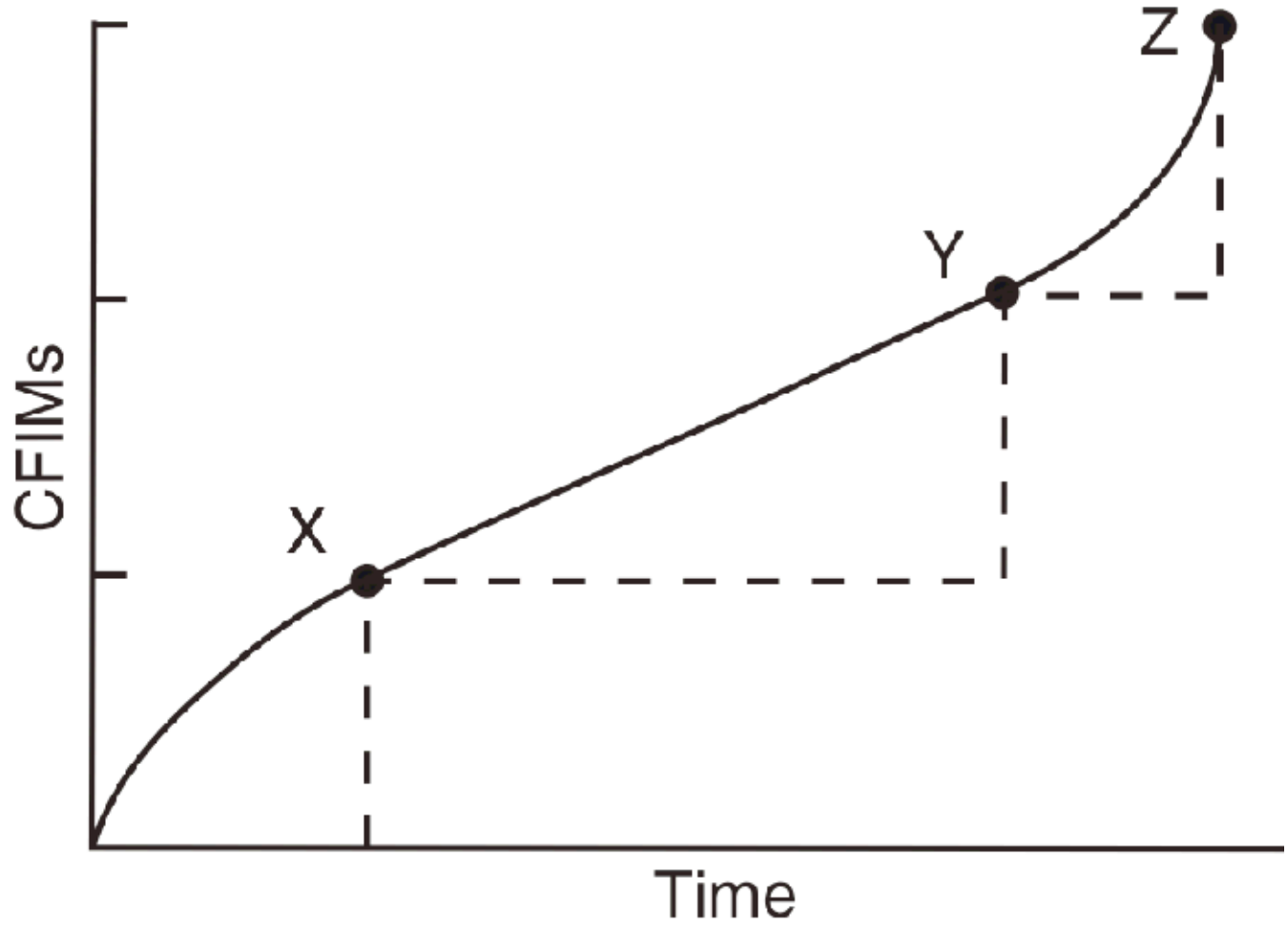
System Day thresholding counts an FDC's CFIMs until the count exceeds a threshold, which generates an alert at the next 5-minute boundary.

The count is then started over, toward creating a new alert for the alert case.

Notice how this type of thresholding differs for:

- *System day* — Each alert covers the amount of time needed to reach threshold.
- *5-minute and hourly* — Each alert covers a 5-minute or hourly period.

Example: In one system day alert case, three alerts, X, Y, and Z appear on the chart below. Each has the same number of CFIMs (above threshold), but some collected CFIMs faster.



Severity

As you can see in the illustration above, where the curve is steepest, the CFIMs are arriving faster, and the problem is more severe.

Based on this information, NTP computes system day alert case severity, which appears in the Asevd field on Ascreen Output.

Tolerance

To compute severity (for the Asevd field on alert cases), NTP uses the TOLERANCE field in the alertperiods table

There is one TOLERANCE for all system day reporting. Default is 60.

Severity is computed as follows:

severity = (minutes between alerts) / (tolerance)

Example:

If ALERT_TOLERANCE variable is...	and it takes this many minutes to generate an SD alert...	Then alert severity is...
60	30	60/30 or 2
	240	60/240 or .25
	2	60/2 or 30

FDC Audit

FDC Audit Feature Overview

Purpose

The optional FDC Audit feature provides a means to audit incoming message types and failure codes (FDCs). The audited data helps determine whether all expected FDCs are being received.

Overview

The feature summarizes all collected FDCs and compares them to the expected results on a network element type basis. You can view the output of the comparison through the BB-GUI, and/or a compiled report available through E-mail.

The expected results are generated by analyzing the existing summary of all FDCs from all targeted network element types and compiling a summary of all the FDCs being collected on a network element type basis. The baseline of expected FDCs is created by analyzing and summarizing the incoming data for 30 days.

All observed FDCs for the targeted network element types are recorded in the baseline table. The administrator can add or delete items in the summary, or mark items as "not to be audited". The expected results can also be re-generated if necessary when new network elements are added to the system.

FDC Audit Tables

The following tables are associated with the FDC Audit feature.

Note: All the tables are viewable via the Find page in the BB-GUI.

Table name	Description
fdc_eqtype	This table defines the FDC values to be audited. **Reference:** See "fdc_eqtype Table" (p. A-69) for details on populating the **fdc_eqtype** table.
fdc_audit	This summary table contains the missing FDC values. **Reference:** For more details, see the *BB-GUI Guide, Appendix A, Surveillance and Summary Database Tables*.

Tables to Edit

Administration of the following tables is required for this feature:

- **swarch** – contains all switches, proper population of **eqtype** is required in order to have retype set correctly in **cfim**,
- **fdc** – contains master list of **fdc**s, used to validate the **fdc_eqtype** table,
- **eqtype** – contains master list of all equipment types, used to validate the **fdc_eqtype** table,
- **fdc_eqtype** – defines the FDC values to be audited; you can update this table on demand.

Setting up Notification

The output of the daily FDC audit can be sent to a list of E-mail addresses and/or files by using the Scheduled Data Distribution feature (described in Appendix A). Parameters can be specified when configuring the E-mail/file output that will filter the specific output, such as one particular switch or all switches in some geographic region.

You can setup notification through the BB-GUI (see "How to Set up Notification" (p. 8-49)).

How to Set up Notification

Purpose

You can set up tabular data output from the Find query page to be sent to destinations such as files and/or E-mail addresses.

Related information

For the background information on Scheduled Data Distribution, see BB-GUI Guide, chapter 5, Analyze, Scheduled Data Distribution.

Before you begin

Important! Before scheduling notification, ensure that:

- your Find search on the FDC audit results is saved,
- the **`bbguiemail`** table contains the list of valid E-mail addresses (populated via **`dbedit`**).

Procedure

Use this procedure to set up notification on the audit results.

1 In the Find output area, click on the **`Schedule`** button.

Result: The configure schedule dialog window is displayed.

2 Select the **`Execution Option`**:

- For the **`Once on`** option, enter a date and time to execute the Find page in the future (you can click the Calendar Dialog icon  to create date entries).
- For the **`Recurring`** option, enter the frequency of execution and a time to execute the report.

3 Select the **`Output format`**:

- For the **`Email list`**, option enter valid user space separated E-mail addresses.

  Note: The list of valid E-mail addresses needs to be populated by the administrator. They are put into the **`bbguiemail`** table (via **`dbedit`**).
- For the **`Output File`** option, the output files are generated in a predefined output storage directory area per user and have 644 permissions.

4 In the title area enter any string as a title for the output.

5 Click on the **Submit** button to add your schedule to the database.

END OF STEPS

Enhanced Mass Call Alerting

Overview

Purpose

Enhanced Mass Call Alerting is an optional feature that provides the ability to generate a mass call alert whenever the CIMs containing the specific digit-fdc pattern cross a system threshold (MCTHRESH) in a given time. It also provides the ability to segregate the alerts by RE so that selected RE groups can be viewed using the network segments feature.

The Enhanced Mass Call Alerting displays alerts on the Alert Cases and Trap Alerts screens.

Contents

Set Enhanced Mass Call variable

MCTHRESH variable

Background information

An additional alert type has been defined called MC (Mass Call). The FQ columns for the MC alert are digits and re. The flexible alerting process uses the MCTHRESH variable to determine the minimum threshold for generating an MC alert.

Purpose

MCTHRESH (Enhanced Mass Call Alert threshold) sets how many CFIMs with the same digits (and LRN) belonging to a specific RE or a set of REs must occur in the same minute before the alert appears on Alert Cases screen output. An MC alert is also viewable on the Trap Alerts screen for every minute in which the alert occurs.

How to use it

To change the MCTHRESH variable, use the following syntax as an example.

```
sui setsys variable=MCTHRESH value=20
```

Reference: For how the Enhanced Mass Call Alerting feature works, see Chapter 4 in the *BB-GUI User's Guide*.

Set FDC screening

Purpose

You can select which FDCs are thresholded or ignored for mass call alerting. To do so, **`dbedit`** the Fdc table and put y (do mass call alerting) or n (do not do it) in the Mc field of each FDC.

Typically, you would put y beside each FDC that is related to mass call problems, such as a "no circuits available" FDC. This screening should have already been done for you when the mass call alerting feature was installed.

Disabling Alerting by Digits

Purpose

Typically, CFIM counts are compared to thresholds, and when thresholds are exceeded, an alert case is created. The Disable Alerting by Digits feature is an optional, purchasable feature that allows you to disable alerting for a given FDC and digit pattern combination. This is useful in "choke network" situations, when calls are intentionally being shed. Disabling a given FDC and digit pattern prevents NTP from generating an unnecessary alert case.

Using the disabledig table

The disabled digit (disabledig) table tells our system which FDC and digit patterns to ignore for alerting. That is, if an FDC and digit pattern is listed in this table, then CFIMs with that FDC and called digit pattern are not tallied into CFIM counts and an alert case is not created.

Use the **dbedit** command to enter an FDC and digit pattern to the disabledig table. The following is a sample entry from the disabledig table:

```
FDC     PATTERN
------- ------------------------------
sva122  3057417539
trans   3102198636
unalloc 1016149391081
```

Important! Any FDC entered into the disabledig Table must first be entered in the fdc table.

Reference: See “disabledig Table” (p. A-57) for more information.

After using the **dbedit** command to edit the disabledig table, enter **ldlkup -f** to load the new table into the system.

Differences between networks

This feature behaves differently for networks using the North American numbering plan (NPA-NXX) versus those who do not.

- For networks using the NPA-NXX plan, if the digits field contains a 7-digit number, the NPA of the distant entity is appended to the digit string, resulting in a 10-digit string. If the distant entity doesn't have an NPA defined in the swarch Table but the reporting entity does, then the NPA of the reporting entity is appended, again resulting in a 10-digit string.

The system then attempts to match based on the disabledig Table. If it finds a match, it sets the peg field to no, and the CFIM will not be included in the alerting counts. If for any reason the string is not 10 digits, no action is taken.

- For networks NOT using the NPA-NXX plan, the system attempts to match based on the disabledig Table regardless of digit field length. If it finds a match, it sets the peg field to no, and the CFIM will not be included in the alerting counts.

The correct numbering plan for your system is specified via the system's numbering_plan parameter during software installation. To change this setting, contact Lucent Customer Support.

Enhanced Mass Call Alerting Feature

Purpose

Enhanced Mass Call Alerting is a solution supporting segmentation between different network groups. Each group can only see data originated or derived from their own set of REs. This solution is different from the standard Mass Call Alert feature where all calls to the same network group were aggregated, regardless of RE.

Important! Enhanced Mass Call Alerting displays alerts on the Alert Cases and Trap Alerts screens.

Reference: For how Enhanced Mass Call Alerting works, see Chapter 4 in the *BB-GUI User's Guide*.

9 Customize

Overview

Purpose

This chapter tells how to modify various system defaults and options affecting what users see, and how the system runs.

Contents

Introduction

Overview

Task overview

Tasks associated with this chapter are as follows.

Task	Description
"Customize the BB-GUI" (p. 9-4)	• The actual port values for Apache, Apache with SSL, and OpenLDAP servers are configurable to help deal with specific environments (see "How to Change Default Port Number for Apache, Apache with SSL, and OpenLDAP" (p. 9-4)). • Any BB-GUI table layouts and saved searches created by a BB-GUI administrator can be accessed by all BB-GUI users. You will most likely want and need to create these for use in the workflow in your organization. • You may want to work with your NTP software (former Network Trouble Patterning) support organization to alter the system defaults for some of the BB-GUI attributes, such as the retention interval for saved searches, font size of displays, and so forth (see "Customize BB-GUI Attributes" (p. 9-7)). • You may want to customize links on the BB-GUI to local or other customer documents. • If your system uses Pattern Painter, you may want to customize the appearance of the Pattern Painter displays (see "Customize Pattern Painter Displays" (p. 9-11)).
"Customize Help Texts" (p. 9-18)	Though NTP typically provides a comprehensive set of FDC's and FDC help text for each conversion, as new FDCs are created, you will want to keep your help text current.
"Customize System Information" (p. 9-22)	Customizing of the system information variables.

Customize the BB-GUI

How to Change Default Port Number for Apache, Apache with SSL, and OpenLDAP

Default Port Numbers

Due to security reasons, the default HTTP, HTTPS, and OpenLDAP port numbers have been set to:

- port **4618** for HTTP connections,
- port **4718** for HTTPS (SSL) connections,
- port **4818** for OpenLDAP connections.

Examples

- Add the following port number to the URL when accessing the BB-GUI:
  http://<host_and_domain>:4618
- If SSL is enabled, add the following port number to the URL when accessing the BB-GUI:
  https://<host_and_domain>:4718

change_port Command

You can change the port number using the **change_port** command.

Syntax

change_port webserver|webserver_ssl|ldap [port]

where:

[port] is the port number that is not already used and must be higher than 1024 (network sockets with numbers below 1024 can be created only by the root user).

Note: If you enter this command without specifying the port number, the system will display the currently used one.

Purpose

The procedure in this section tells you how to change the default port numbers.

Procedure

Use this procedure to change the port number.

1 Log on the 8920 NTP host as ntp.

2 Enter **change_port webserver|webserver_ssl|ldap [port]**

3 Enter **wgui_stop**

4 Enter **wgui_start**

END OF STEPS

Examples

Note: You must be logged in to the 8920 NTP host as **ntp** to proceed:

- Display the currently used webserver port number:
  - Enter **change_port webserver**
    The output is:
    ```
    Currently webserver port is set to 4618
    ```
- Change the OpenLDAP port number to 5555:
  - Enter **change_port ldap 5555**
    The output is:
    ```
    You need to restart BBGUI
    ```
  - Enter: **wgui_stop**
  - Enter **wgui_start**

Create BB-GUI System Table Layouts and Saved Searches

Overview

BB-GUI users as well as web administrators can create table layouts and saved searches.

- All users can access table layouts and saved searches that a web administrator creates.
- Users cannot access each other's table layouts or saved searches.

As administrator, you can create common table layouts and saved searches for the users on your system.

Reference: For the procedures to create table layouts and saved searches, see the *BB-GUI User's Guide*.

Retention duration

NTP stores unused BB-GUI table layouts and saved searches for the retention interval set for the system. The system default retention interval is 180 days (see "BB-GUI attributes" (p. 9-7) for more information on the defaults for these and other BB-GUI attributes).

As long as a table layout or saved search is used within this interval at least once by at least one user, the BB-GUI system retains it. Otherwise, the *cln_bbgui* utility, run out *cron* from the *ntp* crontab file, removes the unused table layout and saved searches (see "ntp crontab File" (p. 2-24)for more information on this utility.)

Important! Do not disable the cron job that runs *cln_bbgui* in an attempt to bypass the system limit on the number of saved searches and table layouts.

Customize BB-GUI Attributes

Overview

Though you cannot change them yourself, your NTP support organization can modify the following attributes of the BB-GUI if necessary for your environment. Contact your NTP support organization for assistance.

BB-GUI attributes

This table describes the default BB-GUI attributes.

Attribute	System Values	Reference
Maximum number of cfim records displayed in the pages of the Pattern Painter feature	Default: 50,000 Maximum: 50,000	For information on Pattern Painter pages, see the *BB-GUI User's Guide* Please note that even if more records are available for display, they are truncated and not displayed.
Maximum number of records retrieved for Find and Compute	Default: 10,000 Maximum: 30,000	See the Max Table Size field in "Web User Administration page parts" (p. 6-39). Please note that the Table Size field (same page) sets the number of records displayed on a page.
Point sizes for font size preferences on BB-GUI pages	Defaults: Small (12), medium (20), large (28), and largest (36)	See the Font Size field in "Web User Administration page parts" (p. 6-39).
Retention interval for saved searches (if searches are not used)	180 days	The *cln_bbgui* utility that runs nightly from the *ntp* crontab file removes old saved searches and table layouts, purges users' histories and logs output. in $LOGDATA. For more information on *cln_bbgui*, see "ntp crontab File" (p. 2-24). For more information on log, see "Monitor BB-GUI Cleanup" (p. 10-40).
Retention interval for table layouts (if layouts are not used)	180 days	
Number of saved searches per user	20	
Number of table layouts per user	20	
Number of BB-GUI users	50	-
Number of pages in autoupdate mode	20	-
Date and time format	Cannot customize.	-

Attribute	System Values	Reference
Length of time a page can be active before it times out.	30 minutes	-

User histories

The number of searches displayed in the user history on each output page is fixed at 25. This is not a tunable BB-GUI attribute. Users never see more than 25 history entries regardless of how many are stored on the BB-GUI server. (See the *BB-GUI User's Guide* for complete information on the functionality of the BB-GUI user history.)

The *cln_bbgui* utility that runs nightly out of cron from the *ntp* crontab file prunes the number of user history entries stored on the BB-GUI server (see "ntp crontab File" (p. 2-24) for more information on *cln_bbgui*).

Important! Do not disable the cron job that runs *cln_bbgui* in an attempt to bypass cleanup of user histories.

Customize data column names

Purpose

Chronological source data column names are configurable by the NTP administrator via a command line command. Once an administrator has changed a data column name the new name appears in place of the original/default column name.

Important! After changing column names of the fields used by *Pattern Painter* a new Pattern Painter template must be created. For information how to create Pattern Painter template, see "Create a Pattern Painter template" (p. 9-13).

Syntax

In order to change data column names use the *change_label* script.

```
change_label  [-c] -t <tablename> [-o <old field name>]
              [-n <new field name>]
```

Parameter	Description
-c	Prompts for the confirmation.
-t <tablename>	Specifies the table name from which the column name will be changed.
-o <old field name>	Original/default name of the column.
-n <new field name>	New name of the column.

Example

```
change_label -t cfim -o re -n re_new
```

Maintain Local Support Links

Overview

The BB-GUI provides links for customers to add their own information to the online documentation pages. The files below are provided as placeholders for customer-defined information.

- The files are in the *$APPLROOT/wgui/html/info/en/custfiles* directory. There is a file for each book in the user documentation set, as well as the Help button, and Customer Support.
- Any file you create should contain:
  - A contact person for the local information
  - A disclaimer stating that information in the file has not been reviewed or verified by Alcatel-Lucent or its representatives.

Files for local support links

This table lists the system default files provided for links to customer-defined information. For current online information on these files and their links, go to the product Launch page, select **Library -> Library Help**, and then select the **Local Practices** link (not the Local Practices button). For information on the Launch page, see the *BB-GUI User's Guide*.

Filename	Description	Go to from
locstoc.html	List of the following files	**Library ->Library Help->Local Practices** button (not the list)
locsupp.html	Customer Support (Comments)	• **Library ->Local Practices -> Customer Support** • **Library -> Local Practices -> Comments**
lochelp.html	Tasks available from the BB-GUI	**Library -> Local Practices ->Help**
locbbgui.html	*BB-GUI User's Guide*	• **Library -> Local Practices and see list** • Tables of Contents for books that are available in HTML • Local Practices Table of Contents
locsa.html	*System Administration Guide*	
loccpadmin.html	*CP Administration and O&M* (used only if your system has CP sources)	

Customize Pattern Painter Displays

Overview

The Pattern Painter feature, which runs in association with the BB-GUI, displays data in graphical form. The graphics include two pie charts and a parabox. Templates determine what CFIM data Pattern Painter graphics include.

Important! The system only provides a default template for the CFIM table. Pattern Painter uses it if no other templates are defined. For tables involved in alerting on the Alert Cases page, you need to define new default templates before running Pattern Painter.

There are three reference tables that you can modify with the **dbedit** command to define the templates:

- "pptemplate Table" (p. A-127)
  This table names the template, defines the CFIM data in the pie charts, and sets the CFIM field that Pattern Painter uses as the primary color field for both the parabox and pie charts.
- "pptemp_columns Table" (p. A-126)
  This table maps an FDC to a template. It defines the data Pattern Painter displays if an Find involves only one FDC.
  This table lists template name, table name, and all the fields Pattern Painter displays in the parabox for a particular template. It also allows you to specify an order for the parabox columns.
  If you delete a template from the pptemplate table, the system automatically deletes that template from the pptemp_columns tables.

  Important! NTP translates all field names and values to lowercase unless there is a specific constraint on a field within the system. In those few instances, the value appears in case-sensitive format. For example, for ease of reading, the Description field retains a mix of upper- and lowercase letters.

Reference

- See **dbedit** in Chapter 3, "Reference Data Tables"
- For information on the CFIM table and Pattern Painter pages, see the *BB-GUI User's Guide*.

Task overview

Use these procedures to administer the Pattern Painter templates.

Task	Procedure
Create templates	"Create a Pattern Painter template" (p. 9-13)
Modify templates	"Modify a Pattern Painter template" (p. 9-15)

Task	Procedure
Delete templates	“Delete a Pattern Painter template” (p. 9-17)

Create a Pattern Painter template

Purpose

Use this procedure to create a Pattern Painter template.

1 Update the pptemplate table to add the new template.

To make a template record for the pptemplate table, enter

sui find source=pptemplate noheader delim = '"|"' maxsave=1 > temp

Result: The file might resemble this:

```
#Template_name|Parabox_col|Column_order|Tablename

default|cpdigits|1|cfim
```

- Use a text editor (such as *vi*) to change the line to define the template you want to add, and then save the file.

It is possible to define parabox columns and mark them for non-display by giving them a column_order of zero (0). This sends information to the specified table, but does not display it initially. The non-display columns can then be accessed through Pattern Painter by selecting them through the parabox. This is useful to compare or refine information with Pattern Painter.

```
#Template_name|Parabox_col|Column_order|Tablename

default|de|0|cfim
```

- To insert the record from the temp file into the pptemplate table, enter
  dbedit -i -f temp -t pptemplate -s '|'
- If you receive a message ending with:
  - "dbedit completed successfully", go to the next step.
  - "Errors saved in file...", see “Correct dbedit Errors” (p. 3-27) .

2 Update the pptemp_columns table to add the new template.

- To make a template record for the pptemp_columns table, enter
  sui find source=pptemp_columns noheader delim = '"|"' maxsave= 1 > temp
  Result: The file resembles this:

```
Template_name|Parabox_col|Column_order|Tablename

default|cpdigits|1|cfim

default|re|2|cfim

default|de|3|cfim
```

- Use a text editor (such as *vi*) to change the lines to define the template you want to add, and then save the file.

  The field defined in a specific template needs to be available in that specific tablename.
- To insert the record from the temp file into the pptemp_columns table, enter

  dbedit -i -f temp -t pptemp_columns -s '|'
- Ensure that the dbedit was successful, as you did in the previous step.

END OF STEPS

Modify a Pattern Painter template

Purpose

Use this procedure to modify a Pattern Painter template.

1 Update the pptemplate table with the modifications.

- To make a template record for the pptemplate table, enter (where the first *name* is the name of the template you want to modify and the second name is the *name* of the table you want to access.)

  sui find source=pptemplate search=template_name=*name* and tablename=*name* noheader delim = '"|"' > temp

  Result: The file resembles this:`444otrltemplate|cfim|cpdigits|digits|etime|testing template|wrb`
- Use a text editor (such as *vi*) to change the line to define the template you want to add, and then save the file.
- To insert the record from the temp file into the pptemplate table, enter

  dbedit -u-f temp -t pptemplate -s '|'
- If you receive a message ending with:
  - "dbedit completed successfully", go to the next step.
  - "Errors saved in file...", see “Correct dbedit Errors” (p. 3-27) .

2 Update the pptemp_columns table with the modifications.

- To make a template record for the pptemp_columns table, enter (where the first name is the *name* of the template you want to modify and the second *name* is the name of the table you want to access.)

  sui find source=pptemp_columns search=template_name=*name* and tablename=*name* noheader delim = '"|"' > temp

Response

The file resembles this:

```
444otr1template|cpdigits|cfim

444otrltemplate|re|cfim

444otrltemplate|de|cfim

444otrltemplate|digits|cfim

444otrltemplate|etime|cfim
```

- Use a text editor (such as vi) to change the lines for the modifications you want, and then save the file.
- To insert the record from the temp file into the pptemp_columns table, enter
  dbedit -u -f temp -t pptemp_columns -s '|'
- Ensure that the dbedit was successful, as you did in the previous step.
  For what to put in each field of the pptemp_columns table, see "pptemp_columns Table" (p. A-126) .

END OF STEPS

Delete a Pattern Painter template

Purpose

Use this procedure to delete a Pattern Painter template.

1 To make a template record for the pptemplate table, enter

```
sui find source=pptemplate search=template_name=name and tablename=name
   noheader delim = '"|"' > temp
```

(where the first *name* is the name of the template you want to delete and the second *name* is the name of the table you want to access).

2 To delete the record in the temp file from the pptemplate table, enter

```
dbedit -d-f temp -t pptemplate -s '|'
```

You do not have to delete the template from the pptemp_columns table. The system does that automatically when you delete the template from the pptemplate table.

3 If you receive a message ending with:

- "dbedit completed successfully", go to the next step.
- "Errors saved in file...", see “Correct dbedit Errors” (p. 3-27).

END OF STEPS

Customize Help Texts

Manage Help Texts

Overview

In the NTP software there are three kinds of help texts:

- FDC help text.
- Column help text.
- Column Tooltips.

Every help text can be managed by a system administrator, see "How to manage help texts" (p. 9-20)

Purpose

As a system administrator, you can manage help texts to:

- Create new help text for column tooltip or new FDCs
- Replace already existing help texts.
- Enabling and disabling one particular or all help text assigned to specified feature.

FDC help text

BB-GUI users can access online help text that explains final disposition codes (FDCs) on any table that contains an FDC field or through the FDC Dictionary link available on the Library Page. Help is also available via the **`sui help`** command.

Reference: *See BB-GUI User's Guide, chapter 2, Getting Started, How to get FDC help.*

NTP provides comprehensive FDC help text for numerous switches and FDCs. The information in the help text comes from standard switch documentation, for example, the *Domestic* and *International Call-Irregularity Maintenance Reference Handbooks* for the *4ESS* and *5ESS* switches.

> **Important!** Maintaining the FDC help is important. If no help is available for an FDC, a user sees the following message:
>
> `No help text is available for the following FDCs: fdc`

Column help text

Column help text shows what a column heading means. There is a column help text for every column in every table in NTP. For information how to get column help, see "describe Command" (p. 3-10) or see *BB-GUI User's Guide, chapter 2, Getting Started, How to get field help.*

Column tooltips

Chronological source data column names have tooltips. The tooltips will appear when the user mouses over the data column name in BBGUI. The default tooltip text is the same as the column name. This applies to any page where chronological source data is visible.

Reference

- For information on the helptext table, see "helptext Table" (p. A-74)
- For a list of CIM types for REs that NTP supports, see the section on where CIMs come from in the *BB-GUI User's Guide* .
- To add or modify an FDC and for background information on FDCs, see "Add or modify an FDC" (p. 4-78) . For information about the fdc table, see "fdc Table" (p. A-68) .

Never Use Ctrl-A inside of Help Text

Never use the ^A character (made by simultaneously pressing the **Control** key and the letter **A** key) inside ofhelp text. Doing so will cause problems. ^A character is an ending character and has to appear only on the end of help text.

How to manage help texts

Overview

Managing help text is possible through command **mod_helptext**. This command allows to creating, replacing, enabling and disabling help texts of FDCs, columns and tooltips.

Enabling or disabling help text

To enable/disable help text, use:

```
mod_helptext enable|disable -t <type>
      [-f <feature>] -k1 <key1> -k2 <key2>
```

To enable/disable all help text for specified feature, use:

```
mod_helptext enable|disable -t <type> -f <feature>
```

<type>, <feature>, <key1>, <key2> are describe on the end of this section in the "Where" block.

Example

To disable the user-defined help text for the no_ans FDC that belongs to the standard FDC group, enter:

```
mod_helptext disable -t fdchelp -k1 no_ans -k2 standard
```

To enable the fdc help text for the pcmd_conv feature, enter:

```
mod_helptext enable -t fdchelp -f pcmd_conv
```

Create or replace user defined help texts

To create/replace user-defined help text from plain text file, use:

```
mod_helptext modify -t <type> -k1 <key1> -k2 <key2> -i <text_file>
```

To create/replace user-defined help texts from csv file, use:

```
mod_helptext modify -t <type> -i <input_file>
```

<type>, <key1>, <key2>, <text_file>, <input_file> are describe on the end of this procedure in the "Where" block.

Example

To modify/add the fdc help text for the no_ans FDC belonging to the standard FDC group (the text is included in the no_ans text file (-i no_ans)), enter

```
mod_helptext modify -t fdchelp -k1 no_ans -k2 standard -i no_ans
```

To add the text stored in the file *column_text* to the digits column help text on the AlertCases page, enter

```
mod_helptext modify -t column -k1 digits -k2 v_acasesum -i column_text
```

To modify the fdc tooltip (the text to be modified is stored in the fdc_text text file) that can be seen on the Find - Alert page, enter

```
mod_helptext modify -t tooltip -k1 fdc -k2 acase -i fdc_text
```

Where:

<type>	<key1>	<key2>	description
fdchelp	fdc	fdcgroup	Values to manage fdc help text
column	fieldname	tablename	Values to manage column help text
tooltip	fieldname	tablename	Values to manage column tooltip

<feature> - the feature name which help text will be enabled/disabled.

<text_file> - plain text file (can be multiline).

<input_file> - csv file with the following format: key1|key2|helptext^A

Example of <input_file>

```
testfdc|testgroup|This is test fdc help text for testfdc fdc^A
```

Customize System Information

systeminfo Table

Purpose

The **systeminfo** table contains the list of variables which present system configuration. The variables in systeminfo table can be customized by **`sysinfo`** command. For reference, see "sysinfo Command" (p. 9-23).

Note: If you want to customize any variable other than described in this guide, we strongly suggest you contact your NTP support organization.

Table structure

Field name	Size	Field description
name	varchar2(40)	This field contains a unique name of the variable.
value	varchar2(200)	This field contains the value of associated variable. The value can be string, integer or boolean.

sysinfo Command

Purpose

The sysinfo command has the following functionality:

- lists all available variables in the **systeminfo** table,
- presents value of the particular variable.
- allows customizing the value of the particular variable.

Syntax

sysinfo

Lists all available variables in the systeminfo table.

sysinfo [-c|-s|-i|-l|-b][-d <dblink>] <name> [<value>]

Parameter	Description
<name>	Name of the variable. If used without <value> parameter presents the value of the variable.
<value>	(optional) Specifies the value which the variable will be set to.
-c|-s|-i|-l|-b	Use one of the following switch to get or set the value as: • **-c** - a character string • **-s** - a short integer • **-i** - an integer • **-l** - a long integer • **-b** - a BOOLEAN (TRUE or FALSE) A character string (-c) is assumed if none of the above options are specified.
-d <dblink>	Use **<dblink>** to identify the remote table.

Example

In the following example we set the *project_name* variable value to 'ntp'

sysinfo project_name ntp

Activate/inactivate the NTP system

Purpose

You can customize the system to stop sending the information from alert notification ("Alert notification" (p. 10-7)) and scheduled data distribution (*BB-GUI User's Guide*) subsystems. The status of the notification subsystems is set in the *sys_active* variable in the "systeminfo Table" (p. 9-22). The valid values are *true* indicating that this is the active system, and false indicating that this is not the active system.

Note: If you create, modify, activate/deactive, or delete a schedule data distribution on the Inactive NTP a message indicating that this action is being done on the Inactive NTP will be presented. Then you will be able to confirm and continue with your changes or cancel with no action taken.

Example

In order to activate/inactivate the NTP system use "sysinfo Command" (p. 9-23).

To inactivate - stop notification subsystems - execute:

```
sysinfo -b sys_active FALSE
```

10 Routine Monitoring

Overview

Purpose

NTP provides log files and other sources of information to help you monitor the system. This chapter explains most of these sources and refers to other parts of the documentation where other sources are explained.

In addition, the procedure to set up responsible parties to receive some types of event notification is included, as are some special corrective actions.

Things to remember

Important! Logs discussed in this chapter are in addition to standard operating system logs, such as */var/adm/syslog/syslog.log* or */etc/rc.log*. See your operating system documentation for information on standard logs.

Contents

Monitoring Recommendations

Task overview

This table gives minimum recommendations for monitoring:

What to monitor	When to monitor
System status via shell commands	At least weekly
System console messages	Continually
Error status messages	When a system console message tells you to, or daily by viewing the err_status file.
Oracle database size	When you receive output from the **chk_space** utility.
Startup and shutdown logs	When the system is installed and after modifications
Boot (initialization) logs	• If the **runstat** command fails to provide information about NTP or Oracle run status • For systems with a CP, if the application is not receiving data from switches for which the CP collects data • For more information than the startup and shutdown logs (see above) provide
maste log admin log	As needed As needed
incon log	Daily
Deletion of old BB-GUI table layouts, saved searches, and user history	As needed
RDS	Each morning (only If you have reference database synchronization)
Links to 8925 Integrated Service Assurance (ISA) and Network Fault Management software [formerly NFM] sources	Daily or as needed
CIM flow from CP (Communications Processor) sources	Daily or as needed
Links via the lnkpm log	As needed
Backup logs	After O&M does weekly backups
CDR error files	Periodically (only if your system receives CDR CIMs), depending on how often you need to reprocesses CDRs for summarization

What to monitor	When to monitor
User databases (user files), accumulation	Periodically and if a "max # extents" message in the master log indicates a space problem

Viewing logs and error files

To browse logs and error files, use the operating system **cat** command or a text editor (such as **vi**). Or where a log may be updated frequently, such as the master log, use the operating **system tail** (enter **Control-D** to stop the **tail**).

Example: This command shows the last 20 lines of a master log and any new lines, as they are logged in the file (where ###.##.## is the log number).

```
tail  -20f  $LOGDATA/maste###.##.##
```

Monitor with Shell Commands

Shell monitoring commands

You can monitor the NTP host by entering operating system and NTP shell commands at the command line.

Examples

This table lists some of the commands you can use for monitoring.

The **root** and **ntp** logins can execute these commands.

Enter	Look for	Reference
ps -ef	Processes that may be hung	Operating system command reference manual
sar	System performance problems	
bdf	File system space problems on the NTP host	
runstat	NTP processes that are running, or not running	"Verify NTP Run Status" (p. 2-3)

Monitor System Console Messages

Console messages

The following types of messages come to the NTP system console:

- Operating system error messages
- NTP system initialization messages
- Critical and major software errors

Important! The system initialization and software error messages are sent with SOM (start of message) and EOM (end of message) characters at the beginning and end of the messages.

CompuLert

The system initialization and software error messages can also be sent to CompuLert or a similar computer monitoring system. You can control the volume of messages sent to the NTP host console via CompuLert control commands.

Alert notification

Purpose

Important! Alert Notification is an optional feature. Contact your Alcatel-Lucent Account Representative for more information.

The Alert Notification feature is based on the NTP find functionality and allows analysts and network managers to be made aware of critical network events without having to actively monitor NTP.

The Alert Notification feature uses the NTP **`notify`** functionality to send a notification using::

- Email,
- an entry in a logfile,
- the UNIX wall and NTP bbgui_notify commands,
- a user created script or program.

Important! You can activate or inactivate the whole alert notification subsystem to stop sending notification. For reference, see "Activate/inactivate the NTP system" (p. 9-24).

Uses of Alert Notification

The Alert Notification feature uses the **`sui find`** command (see "sui find Command" (p. B-18)) to create an alert. If the **`sui find`** command finds one or more matching records, that is considered to be an alert and the results are sent to a user using one of the above specified methods.

Since it uses the **`sui find`** command, Alert Notification can generate an alert on any table but it is primarily intended for the alerting tables, such as alert or acase, or one of the associated views, such as v_acase.

Create an Alert Notification

In order to create an Alert Notification, you will need to create a **`dbedit`** file to populate the alert_notify table (see "alert_notify Table" (p. A-16)). This assumes that you have already created a notify record in the notify table (see "notify Table" (p. A-114)).

The alert_notify table has the following fields:

- Alertname - a unique identifier for this alert notification.
- Searchexp - a search expression suitable for use with the **`sui find`** command.
- Notify_id - a valid notify identifier from the notify table.
- Tablename - the table to be searched using the **`sui find`** command.
- Format - a format expression suitable for use with the **`sui find`** command.
- Runflag - either 'y' if the alert notification is active or 'n' if it is not.

- Delimiter - a delimiter for use with the **sui find** command.
- Repeattime - how often, in minutes, the alert notification should be run.
- Subject - used as the subject for any email sent for the alert notification.
- Lastalert - the last time this alert notification generated an alert.
- Owner - the user who created this alert notification.

The format, delimiter, subject, lastalert and owner are optional and can be left as null values.

Sample Alert Notification dbedit file

In the following example **dbedit** file for *notify* table, we create a notify that sends mail to *piotr*. In the example of **dbedit** file for *alert_notify* table, we create an alert notification called *alert1* that looks in the **acasesum** table for an *acase* with a DE value of *pcmd** and an FDC of either *mobfail* or *swfail* and sends the DE, FDC and CAI values to a notification called *my_notify_id* using the ';' character as the delimiter. This alert notification will be generated no more often than every 15 minutes. Since the *my_notify_id* sends an email, the subject line for the email will be *notification for alert1*. The alert notification is active and is owned by a user called *anuser1*.

```
notify table file for dbedit:
#Notify_id|Notify_type|Severity|Addressee
my_notify_id1|mail|major|piotr.stpiczyński@alcatel-lucent.com

alert_notify file for the dbedit:
#Alertname|Searchexp|Notify_id|Tablename|Format|Runflag|Delimiter|
  Repeattime|Subject|Lastalert|Owner
Alert1|(de=pcmd*) and (fdc=mobfail,swfail)|my_notify_id1|acasesum|
  de:12,fdc:7,cai:5|y|;|15|notification for alert1|-|anuser1
```

Disabling and Deleting Alert Notifications

A single alert notification can be disabled by setting the runflag for the alert notification to 'n'. If you want to delete the alert notification, use the same **dbedit** file used to create the alert notification or generate a new **dbedit** file using the **sui find** command. For more information on using **dbedit**, see "dbedit Command" (p. 3-22).

Notify Feature

The notify feature provides NTP command with an orderly and consistent way to communicate useful information to users of NTP, either internal or external.

Command Syntax

The notify command supports two commands line formats:

- **notify -i <notify_id> -m <message> [-s <subject>]**
- **notify -i <notify_id> -f <message file> [-s <subject>]**

In both cases, the you must provide a notify_id from the notify table and may, if desired, provide a subject. You must also provide either a file name containing the message to be sent, or the actual text of the message.

The **notify** command uses a **notify** table to hold information on users, both external and internal, who can receive data from NTP, the method by which the information will be sent, the severity or importance of the data and, if applicable, the address or location of the user. For reference of the structure of the **notify** table, see: "notify Table" (p. A-114)

Note: When alert notification is using the *prog* type of the notify, a user created script or program will be called with the following parameters **-i <notify_id> -f <message file>**

autotest Tool

Overview

The autotest tool provides a method of monitoring system status and health. Autotest will automatically (via cron) run a default series of tests to check various parts of the system. In addition, users can create their own configuration files to be executed by autotest.

Two Ways to run autotest

By default, the autotest tool is set up to run a default set of tests (or configuration files) from the cron file (see "ntp crontab File" (p. 2-24)). Users can also run autotest as a command on their own configuration files (see "autotest command" (p. 10-10)).

Default Tests

The default tests are:

- current_alerts — verifies that alerts are coming into the system and being processed.
- current_cfims — verifies that CFIMs are coming into the system and being processed.
- current_cims — verifies that CIMs are coming into the system and being processed.
- current_falerts — verifies that falerts are coming into the system and being processed.
- filesystem_space — checks whether the NTP filesystem is becoming full.
- process_respawn — alerts if an NTP process has been respawned.
- system_running — verifies that the NTP application is up.
- check_sources — creates a test for every source on the system. These created tests are called current_*<source name>* and verify that the indicated source is providing data.

autotest command

autotest *<configuration file name>*

Any created or modified configuration files should be in the *$USERDIR/test* directory.

Creating a Configuration File

You can create your own configuration file to run a command or test automatically with cron. This is an example of an autotest configuration file. The valid field entries are detailed below.

```
NAME=current_cfim
   COMMAND=cur_cfim
   ARGS=
   NOTIFY_TYPE=mail
   MAIL_LIST=${APPLOWNER:-ntp}
   ALERT_LEV=major
```

Field	Valid Values
• NAME	• The name of the test (this appears in the event_status table and any notification sent to the user).
• COM-MAND	• The command that implements the test. Any valid command that returns zero on success and a number on failure is allowed. (For example, "vldopt".)
• ARGS	• The desired arguments for the command.
• NOTIFY TYPE	• Type of notification to be sent. Values are: mail, wall, log, none.
• MAIL_LIST	• Comma separated list of email addresses. Used only if the notify_type is mail.
• ALERT_ LEV	• Alert level. Values are: critical, major, minor, none.

Sample Output

This is an example of autotest results as shown in the event_status table on the BBGUI. It reports, for example, that system_running and several others executed and passed, but current_falerts failed.

Analyze Table Name=event_status, Host=135.7.37.74, User=NetAdmin

Search: Query Aggregate History

45 Records

ID	fail_cnt	last_fail	last_run	name	status
1	0	03/03/07 13:48	03/03/07 14:13	system_running	pass
2	0	03/03/06 13:10	03/03/07 14:10	process_respawn	pass
3	0	03/03/07 13:45	03/03/07 14:10	current_cfim	pass
4	0	03/03/07 13:45	03/03/07 14:10	current_cims	pass
5	1	03/03/07 13:46	03/03/07 13:45	current_falerts	fail

This is an example of a wall message sent as a result of autotest:

```
Broadcast Message from ntp (pts/1) Fri Mar  7 14:53:15...
critical: test system_running failed at 03/07/03 11:26:04
```

Additionally, output can be directed to mail or the log file.

Monitor Oracle Database Size

Overview

The *chk_space* utility runs out of *cron* (see "NTP-related crontab files" (p. 2-20)). It monitors the Oracle tablespaces and checks the data files associated with them. If a data file is getting too full, *chk_space* may do the following:

- Add a new data file for that tablespace. Maximum space allocated for each data file is 2 Gb.
- Log a message in the master log (see "master Log" (p. 10-25)).
- Send a message to the responsible parties set in the notify table (see "Alert notification" (p. 10-7) If nobody is specified in the notify table to receive messages, by default *chk_space* sends a message to the ntp login ($APPLOWNER).

The message may include information on the amount of free disk space, the sizes of the various database files, and an indication if the size of any tablespace has been increased.

Output

The *chk_space* utility ensures that the application filesystem (*/lucent/ntp*) has sufficient free space and that the application database is not consuming too large a percentage of the application filesystem. In addition, for the chronological tablespaces (those listed in the chron_info table), the *chk_space* utility attempts to estimate how much space the tablespace will require in order to hold the desired number of days of data as specified in the chron_info table. Since some tablespaces hold more than one data table, the total number of days for all tables in the tablespace are used in the estimate.

Example: Both the acase and acasesum tables are stored in theacase tablespace. When estimating the growth for the acasetablespace, the total days specified for both tables are addedtogether.

Output from the chk_space utility resembles the following:

```
/lucent/ntp:
   Total MB:        378981
   Total MB used:   159352
   Total MB avail:  219629
Tablespace ACASE is using 92 MB
Tablespace ADMUSER is using 268 MB
Tablespace ALERT is using 136 MB
Tablespace ARCHIVE is using 20 MB
Tablespace BILLDATS1 is using 40 MB
Tablespace BILLDATS2 is using 40 MB
Tablespace CFIM1 is using 1120 MB
Tablespace CFIM2 is using 1080 MB
Tablespace CIM1 is using 920 MB
Tablespace CIM2 is using 920 MB
Tablespace ICFIMIDX1 is using 310 MB
```

```
Tablespace ICFIMIDX2 is using 310 MB
Tablespace INDX is using 60 MB
Tablespace LINKALERT is using 225 MB
Tablespace OTRSUMM is using 1 MB
Tablespace REFERENCE is using 102 MB
Tablespace SUMMCOUNT is using 771 MB
Tablespace SYSTEM is using 200 MB
Tablespace THRESH is using 5 MB
Tablespace THRESHOLDING1 is using 120 MB
Tablespace THRESHOLDING2 is using 120 MB
Tablespace USR is using 60 MB
The total database size is 6920 MB
Tablespace group acase must extend by 33 MB
   acase has 73 days stored and requires 100 days
Tablespace group linkalert must extend by 3 MB
   linkalert has 12 days stored and requires 13 days
Tablespace group summcount must extend by 3142 MB
   summcount has 1040 days stored and requires 5285 days
Tablespace group thresholding must extend by 22 MB
   thresholding has 54 days stored and requires 62 days
Total database growth required is 3200 MB
Total filesystem space available is 219629 MB
```

Corrective action

Take precautions to prevent the system from running out of space.

- If disk usage for chronological database files, such as cfims, cims, otr, and alert, etc.) is too great, contact your NTP support organization for help in reducing the retention interval for this type of data.
- The system has many checks to clean out unnecessary data. As a general rule, whenever *chk_space* adds a new data file, you should determine why and if it is acceptable.

Monitor NTP Startup and Shutdown

Overview

Monitor system startup and shutdown to see if surveillance data was lost due to unscheduled shutdowns or if there are problems running the NTP and the runstat command does not provide output (see "runstat command" (p. 2-3)). You would probably monitor startup and shutdown weekly, or when you anticipate problems, such as during the first weeks after installation or NTP software updates.

- The monthly logs list shutdown and startup events.
- The boot (initialization) logs provide more detailed information. We recommend you do this before contacting your NTP support organization in the event of a problem running NTP. The boot log for CP processes may be useful if NTP is not receiving data from a switch for which the CP is a collector.

Monthly logs

For each of the last 12 months, the system has a monthly log file listing manual and automatic system startups and shutdowns. These log files are:

- In the $WORKDIR/run directory.
- Named log.*mm* , where *mm* is the month (01 for January, and so on).

Format of monthly logs

Entries in the monthly log files resemble the following, and have two or three parts, as explained in the table:

```
09/09/03 13:45:47 MANUAL-STARTUP

   09/09/03 13:46:00 MANUAL-SHUTDOWN elapsed seconds: 13
```

Part	Function
Date and time.	Tells when the system started up or shut down.
Either: • MANUAL-SHUTDOWN • MANUAL-STARTUP • AUTO-SHUTDOWN • AUTO-STARTUP	Tells whether the application: • Was manually shut down with the **ntpstop** command • Was manually started up with the **ntpstart** command • Had an unrequested shutdown, due to a software failure • Started up automatically when the system was booted (from the boot program called **ntpstart**)

Part	Function
Elapsed seconds	Tells how many seconds the system was up prior to a shutdown (for MANUAL-SHUTDOWN or AUTO-SHUTDOWN entries only).

Boot logs

Startup and shutdown messages are logged in the order shown here:

1. *$WORKDIR/boot/BOOTLOG* — for Oracle processes and NTP daemon processes
2. *$WORKDIR/run/INITLOG* — for the NTP application
3. *$SCPDIR/run/INITLOG* — (optional) for CP processes, if your system has a CP collector.
   For a standalone CP, this log is on the CP machine as */opt/scp/run/INITLOG* (see "CP Software, Files, and Databases" in Chapter 2 of *CP Administration and O&M*).

scp INITLOG

If your system has a CP, the $SCPDIR/run/INITLOG file logs messages for the last CP startup or shutdown. INITLOG.old logs messages for the startup or shutdown previous to that. This log may be helpful in cases where NTP is not receiving data from switches for which the CP collects data.

Important! On a standalone CP, this file is opt/scp/run/INITLOG.

Example for normal startup

For a normal startup, this file should show the system going to run level 4.

```
08/21 17:23:54 BEGINNING STARTUP SEQUENCE

08/21 17:23:54 Going to run level 4

RUNNING COMMUNICATION PROCESSOR SOFTWARE

LOGDAEMON RUNNING!

 + Starting autonomous processes

 + Autonomous processes started
```

Example for normal shutdown

For a normal shutdown, this file should resemble the example above with additional lines like the following:

```
08/21 16:55:50 SHUT-DOWN REQUESTED

08/21 16:55:50 BEGINNING SHUT-DOWN SEQUENCE: PLEASE WAIT...

08/21 16:55:50 Going to 'shut-down' run level

08/21 16:56:00 SHUT-DOWN SEQUENCE COMPLETED

08/21 16:56:00 Terminating!
```

Oracle BOOTLOG

$WORKDIR/boot/BOOTLOG logs messages for the last startup or shutdown. BOOTLOG.old logs messages for the startup or shutdown previous to that.

Example for normal startup

For a normal startup, this file should show the system going to run level 5.

```
06/14 18:09:20 BEGINNING STARTUP SEQUENCE

06/14 18:09:20 Going to run level 5

RUNNING <application> BOOT PROCESSES

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Copyright (c) 1989-200x Alcatel-Lucent.  All rights reserved.


THIS IS UNPUBLISHED PROPRIETARY SOURCE CODE OF Alcatel-Lucent.

 The copyright notice above does not evidence any actual or

         intended publication of such source code.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

LOGDAEMON RUNNING!

Oracle listener already started

Oracle already started

 + Boot processes started

06/14 18:11:20 Going to run level 5
```

Example for normal shutdown

For a normal shutdown, this file should resemble the example above with additional lines like the following:

```
08/25 11:19:23 MANUAL-SHUTDOWN

08/25 11:19:23 BEGINNING SHUT-DOWN SEQUENCE: PLEASE WAIT...

08/25 11:19:23 Going to 'shut-down' run level

08/25 11:19:39 SHUT-DOWN SEQUENCE COMPLETED

Oracle listener stopped

Oracle stopped

08/25 11:21:10 Terminating!
```

NTP INITLOG

$WORKDIR/run/INITLOG logs messages for the last startup or shutdown. INITLOG.old logs messages for the startup or shutdown previous to that.

Example for normal startup

For a normal startup, this file should show the system going to run level 5 and deleting cached database information so it can be refreshed later. If there are errors, you will see them as indicated in the example.

```
11/29 09:23:48 BEGINNING STARTUP SEQUENCE

11/29 09:23:48 Going to run level 5

RUNNING ntp SOFTWARE

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Copyright (c) 1989-200x Alcatel-Lucent.  All rights reserved.


THIS IS UNPUBLISHED PROPRIETARY SOURCE CODE OF Alcatel-Lucent.

 The copyright notice above does not evidence any actual or

          intended publication of such source code.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

l.* not found

 + Starting autonomous processes

Initializing Flexible Alerting tables

Table created.

Index created.

Table analyzed.

Table created.

Table created.

Initialization of Flexible Alerting Tables completed

 + Autonomous processes started

EXECUTION ENVIRONMENT RUNNING

11/29 09:24:44 Going to run level 5
```

Example for normal shutdown

```
For a normal shutdown, this file should resemble the example

   above with additional lines like the following:

08/25 11:19:16 MANUAL-SHUTDOWN

08/25 11:19:16 BEGINNING SHUT-DOWN SEQUENCE: PLEASE WAIT...

08/25 11:19:18 Going to 'shut-down' run level

08/25 11:19:20 SHUT-DOWN SEQUENCE COMPLETED

08/25 11:19:22 Terminating!
```

Monitor Application Logs ($LOGDATA)

Overview

Application logs are chronological files automatically generated by the NTP application. They are flat files in ASCII format, stored in the $LOGDATA directory.

Application logs

NTP maintains the following log files for application events.

$LOGDATA file	Description
maste	Includes all application error and information messages
admin	Lists the most important error and information messages
incon	Records inconsistencies among incoming data and NTP reference tables
lnkpm	Lists errors from source links
rel_intern_err	Records internal errors logged by the event logger
sccs	Contains messages from ISAs (CIMS not in correct format)
backup	Contains backup logs for NTP
univlog	Messages from universal switches (CIMs not in correct format)
cln_bbgui	Lists expired BB-GUI saved searches, table layouts, and user histories that the system will delete

Important! The $LOGDATA directory also contains the following files used by your NTP support organization. These files are created by the *err_log.sh* utility that runs out of cron (see "ntp crontab File" (p. 2-24)). You do NOT need to monitor these files.

- uniq_incon_*hostname* _err
- uniq_maste_*hostname* _err

Retention interval

The logs are rolled over as new logs are generated. The system retains:

- Six lnkpm log files
- Three files each of all other logs

Log file naming

NTP logs, except rel_intern_err, have two parts in their names:

- The first part is a string, either: maste, admin, incon, or lnkpm.
- The second part is the date and time, in NNN.HH.MM format, when the file is created, where:
  - *NNN* is the julian date (Example: January 1 is 001).
  - *HH* is hour of the day, in 24-hour format, when the first event of the day was logged (Example: 4 p.m. is 16:00).
  - *MM* is the minute when the first event of the day was logged.

Example: If the master file logged its first event at 2:30 a.m. onAugust 22, the name of the file would be maste234.02.30.

Log message header example

Here is an example of a typical header on a message in an application log file.

```
Mon Jan 27 15:44:35 2003 HP-UX:9000/891:LOGDAEMON
   logdaemon.c:1104
LOG001  LG_START_LOG  ** START OF LOGFILE
   '/logdat/maste027.15.44' ** openDest
```

Message headers

Each message in an NTP log file is preceded by a header identifying the message. The fields of the header typically include:

- Severity level of problem
- Day message was generated
- Date message was generated
- Time message was generated
- Year message was generated
- Machine address
- Operating system
- Process name
- User (login) that invoked the process
- Location of error in software (C file)

Severity levels

The severity levels in NTP logs are as follows:

Level	Indicated by this before time and date	Meaning
Critical	*C	The error may have caused the system to crash or become inoperable (for example, head crash, autonomous process initialization failure, autonomous process death). Failure to restart will halt some significant operations.
Major	**	Hardware or software failures that make the system partially inoperable (for example, corrupted shared memory table detected, important IPC message cannot be delivered). These inconsistencies are not serious enough to halt execution but are too important to be ignored. Such errors, if not corrected, make the system ineffective in future operations.
Minor	*	Errors that probably do not make the system inoperable and are usually made by users (for example, erroneous entries). The system responds by an error message.
Info	blank	Informational events (for example, the start of an autonomous process).

master Log

Purpose

This file (or files) is a chronological log of NTP critical, major, and minor errors and general informational events.

The files are named maste*julian date.hour.minute* , for example: maste283.14.16

Hint: See "Application logs" (p. 10-22) *for other files in $LOGDATA.*

Important! Errors generated by **`dbedit`** are logged in the master log.

Creation/ removal

A new master file is created when the current file reaches 100k bytes. Each file is automatically removed after 14 days.

Message format

Each message in the master log has two lines, with the following information:

```
Severity Date_Time Software_module File Line
    Message_number Error_message
```

Message parts

This table lists the fields of the master log messages.

This part...	Tells you...
`Severity`	See "Severity levels" (p. 10-24) .
`Date_Time`	When the message occurred
`Software_module`	Where in the system the message was detected
`File line`	Program producing error and line number of code
`Message_number`	Application message number
`Error_message`	Text message

Examples

The following are examples of master log messages.

```
*  Tue Jun 24 03:15:35 2003 HP-UX:9000/891:io_tsm1:ntp DataPort.C:
   202
ERR001 Source 'tsm1' link timed out. Closing port.

   Tue Jun 24 03:18:45 2003 HP-UX:9000/891:io_tsm1:ntp Dkport.C:501
ERR002 EVENT Opening port for source 'tsm1'

*  Tue Jun 24 04:46:11 2003 HP-UX:9000/891:io_tsm2:ntp DataPort.C:
   202
ERR001 Source 'tsm2' link timed out. Closing port.

   Tue Jun 24 04:49:21 2003 HP-UX:9000/891:io_tsm2:ntp Dkport.C:501
ERR002 EVENT Opening port for source 'tsm2'

   Tue Jun 24 07:59:47 2003 HP-UX:9000/891:io_tsm2:ntp CimPtr.C:435
```

admin Log

Purpose

The admin log is a chronological log of critical and major errors. It is a subset of messages in the master files. See "Severity levels" (p. 10-24) for severity levels.

Hint: See "Application logs" (p. 10-22) *for other files in $LOGDATA.*

Creation/ removal

A new admin file is created when the current file reaches 100 Kbytes. Each file is automatically removed after 14 days.

Message format

Each message in the admin log has two lines, with the following information:

```
Severity Date_Time software_module file line
   message_number error_message
```

Examples

The following are examples of admin log messages.

```
   Thu Jun  5 00:16:05 2003 HP-UX:9000/891:LOGDAEMON logdaemon.c:
  1104
LOG001  LG_START_LOG  ** START OF LOGFILE '/logdat/admin156.00.16'
  ** openDest
** Thu Jun  5 00:16:05 2003 HP-UX:9000/891:io_cp1:ntp SendMsg.C:68
ERR001 queue='samp_rate_mon', type=1016, size=677, stat=1, (errno=
  11)

** Fri Jun  6 00:16:08 2003 HP-UX:9000/891:io_cp1:ntp SendMsg.C:68
ERR001 queue='samp_rate_mon', type=1016, size=515, stat=1, (errno=
  11)

** Sat Jun  7 00:16:16 2003 HP-UX:9000/891:io_cp1:ntp SendMsg.C:68
ERR001 queue='samp_rate_mon', type=1016, size=623, stat=1, (errno=
  11)

** Sun Jun  8 00:16:14 2003 HP-UX:9000/891:io_cp1:ntp SendMsg.C:68
ERR001 queue='samp_rate_mon', type=1016, size=677, stat=1, (errno=11)
```

Reference

The incon log is a file located in $LOGDATA. See "Monitor Application Logs ($LOGDATA)" (p. 10-22) for general information about $LOGDATA.

incon Log

Purpose

The incon (inconsistency) log is a chronological log of:

- Inconsistencies between NTP record bases and matrices
- Inconsistencies between CP record bases and NTP's (if your system uses CP sources)
- Invalid status messages received from 8925 Integrated Service Assurance (ISA)
- Problems with CIMs in files of CDR CIMS that might

References

For other files in $LOGDATA, see “Application logs” (p. 10-22)

If a log entry contains the word "geoprobe", see “Fix GeoProbe Problems in incon Log” (p. 10-45) .

Creation/removal

All but the latest three files are removed each night.

Examples

The first two incon messages below indicate that FDCs are undefined in the fdc table.These messages include the entire CIM. The last two messages indicate omissions from the dmsroute and swarch tables, respectively, and do not include the entire CIM.

```
Wed Apr 19 07:05:08 2003 HP-UX:9000/889:io_egh02:ntp Incon.C:125
ERR002 EVENT ORG_DMS "TRK352" RE londen0400t FDC TRK352 not in "fdc"
  table. Msg discarded.
Msg=05 TRK 352 9044 INFO TUP TRK TRBL CKT     VIDESUPDM2W 446
       REPORTING CKT     VIDESUPDM2W  446
       REASON = INVALID SHP CPI COMB
       CIC = 446  SHP = 0  CPI=1
   Sat Apr 22 08:10:12 2003 HP-UX:9000/889:io_egh02:ntp Incon.C:125
ERR002 EVENT ORG_DMS "LINE138" RE eghmen0100t FDC LINE138 not in
  "fdc" table. Msg discarded.
Msg=10 LINE138 1384 INFO TRMT CKT     VIBRUSET2W   75
       TREATMENT SET = UNDT   CALLED NO = 31786151427
       CALLID= 3FA9 001F
   Tue Jun 20 12:56:20 2003 HP-Utsm3X:9000/891:io_tsm3:ntp DeDms.C:
  439
ERR002 EVENT RE = svstohxxcg0, TGCLLI = ROTLTP not in "dmsroute"
  table.

   Tue Jun 20 12:58:41 2003 HP-UX:9000/891:io_cp1:ntp Incon.C:121
ERR002 EVENT No HNPA for "clmbohxxcg0" in swarch.
```

Important! The "tsm" in the messages above means ISA.

Corrective actions

This tables references known corrective actions:

Entry in incon log	Possible meaning	See
The FDC begins with lnp, and eqtype is 5ess or ewsd.	The FDC is not defined.	
For any configurable converter CDR CIM	You may want to reprocess the CDR	“Assign or Modify FDC Group and Network Group/Segments for BB-GUI Users” (p. 7-28)

lnkpm Log

Purpose

The lnkpm log collects link status messages regarding CIM sources. They are useful for troubleshooting the links to new sources that you add to NTP and for determining the health of existing links.

Reference

- See "Application logs" (p. 10-22) for other files in $LOGDATA.

Creation/removal

All but the latest three files are removed each night.

Monitoring lnkpm

Rather than monitor lnkpm, it is better to use either of the following:

- **`sui linkmon`** (see "Syntax for dbedit" (p. B-20))
- **`sui find so=linkstatus se=status!=up`** (see "sui find Command" (p. B-18) for a complete list of **`sui find`** options and arguments)

Example: General CIM messages

Messages with "CIM" following the date and time are 5-minute summaries of CIM activity on the link. The fields following "CIM" report the number of CIMS that NTP:

- Processed (received and recognized) in the past 5 minutes
- Could not convert to CFIMs and therefore discarded (due to a lack of either an re or FDC in the CIM)
- Dropped because the message queue in the CFIM converter was full.

```
Mon Jun 23 23:00:17 2003 HP-UX:9000/891:io_tsm2:ntp

   IOStats.C:120

ERR002 EVENT 06/23/03 23:00 CIM tsm2 4 0 0



Mon Jun 23 23:00:17 2003 HP-UX:9000/891:io_tsm3:ntp

   IOStats.C:120

ERR002 EVENT 06/23/03 23:00 CIM tsm3 7 0 0
```

Example: General link status messages

General link status messages report the name of the source sending the message and include the text string of the status message as received. Messages in this log include switch-source messages, source -NTP messages, and unrecognized messages.

This example shows messages for an 8925 Integrated Service Assurance (ISA) source (both "sccs" and "tsm" in the messages mean ISA).

```
Sun Jun 22 05:56:00 2003 HP-UX:9000/891:io_tsm3:ntp LsmIfcSCCS.C:201

ERR002 EVENT SCCS_STATUS msg from 'tsm3':

   'CLMBOHXXCG0  57 REPORT LOG STATUS 120 Removed logging : SRC
  wnc110c.mtc'

   (link down assumed)

   Sun Jun 22 05:56:04 2003 HP-UX:9000/891:io_tsm3:ntp LsmIfcSCCS.C:
  201

ERR002 EVENT SCCS_STATUS msg from 'tsm3':

   'CLMBOHXXCG0  57 REPORT LOG STATUS 119 Restored logging : SRC
  wnc110c.mtc'

   (unrecognized)
```

Example: Port messages

Messages with "DK" following the date and time are hourly summaries of activity on the port. The fields following "DK" report the:

- Source name (from the name field of the source table)
- Total number of messages on the link in the past hour
- Total number of reframes in the past hour
- Number of times the Datakit or TCP/IP port was closed in the hour

This example shows a general log message:

```
Sun Jun 22 06:00:17 2003 HP-UX:9000/891:io_tsm1:ntp

  IOStats.C:94

ERR002 EVENT 06/22/03 06:00 DK tsm1 3489 0 0

Sun Jun 22 06:00:18 2003 HP-UX:9000/891:io_tsm2:ntp

  IOStats.C:94

ERR002 EVENT 06/22/03 06:00 DK tsm2 2240 0 0

Sun Jun 22 06:00:19 2003 HP-UX:9000/891:io_tsm3:ntp

  IOStats.C:94 ERR002 EVENT 06/22/03 06:00 DK tsm3 578 0 0
```

Example: RE-CP link messages

lnkpm messages with "RE" following the date and time report the status of a switch-CP link. The fields following the "RE" show the:

- Reporting entity link this message is about
- CP reported to by this reporting entity
- Number of messages received from this reporting entity by this CP
- Percent of unreadable messages received
- Percent of messages received with lost data
- Number of link failures
- Status for the RE-CP link as received in link status message
- Link status as derived by the application from other data and the thresholds set in system variables.

```
Wed Oct 7 09:00:17 2003 wisvb:vax:lsm_c1s2 procMsgs.C:333

ERR002 EVENT 10/07/92 09:00 RE dllstxt134t kscy1 12 0 0 0 - -


Mon Jun 23 23:01:42 2003 HP-UX:9000/891:lsm:ntp ReCpLnk.C:267

ERR002 EVENT 06/23/03 23:01 RE clmbohxxcg0t cp1 81 0 0 0 up up


Mon Jun 23 23:01:42 2003 HP-UX:9000/891:lsm:ntp ReCpLnk.C:267

ERR002 EVENT 06/23/03 23:01 RE clmbohyycg0 cp1 101 0 61 0 up

   up
```

Example: CP-NTP link messages

lnkpm messages with a "CP" following the date and time report the status of a link between a CP and NTP (if your system uses a CP source). The fields following the "CP" show the:

- CP that sent this link status message
- Date and time the last message from the CP was received
- Number of messages dropped by the CP due to link overflow
- Number of messages dropped by the CP due to link error
- Status for the link
- Link status as derived by NTP from other data and the thresholds set in system variables.

```
Wed Oct 7 09:00:17 2003 wisvb:vax:lsm_c1s2 procMsgs.C:299

ERR002 EVENT 10/07/92 09:00 CP clmb1 10/07/96 09:31 0 0 - -
```

sccs Log

Purpose

The sccs log collects critical and major event messages from ems-type CIM sources regarding CIMS with incorrect format. Entries include the entire CIM. Entries in this log are a subset of the messages in the maste log.

Reference

- See "Application logs" (p. 10-22) for other files in $LOGDATA.

Creation/removal

A new SCCS file is created when the current file reaches 100k bytes. Each file is automatically removed after 14 days.

Example

This example shows sccs messages.

```
Thu May  4 01:18:28 2003 HP-UX:9000/889:io_egh02:ntp SCCSMsg.C:303

ERR002 EVENT 'egh02' invalid msg: 01TOROONJYDS0

  18 C7UP105 4367 INFO UNSUCCESSFUL CALL ATTEMPT

        CKT     TORNYC_IMT 1605

        REPORTED BY CKT     TORNYC_IMT 1605

        REASON = UNALLOCATED NUMBER

        ROUTESET =       C7RTTORONY

        CLDNO = 5042358874

   Thu May 4 01:18:35 2003 HP-UX:9000/889:io_egh02:ntp SCCSMsg.C:303

ERR002 EVENT 'egh02' invalid msg: 01TOROONJYDS0

  18 C7UP101 4468 FLT  UNREASONABLE MSG RECEIVED

        ORIG CKT     TORNYC_IMT 1610 TERM

        REPORTED BY CKT     TORNYC_IMT 1610

        REASON = UNREASONABLE MSG ON IDLE CKT

        RECEIVED MSG 0130 SUBTYPE 0009

   Thu May  4 01:18:57 2003 HP-UX:9000/889:io_egh02:ntp SCCSMsg.C:
  303

ERR002 EVENT 'egh02' invalid msg: 01TOROONJYDS0

  19 TRKT212 5276 INFO TRMT CKT   HNGKNGIMTTOR   15

        TREATMENT SET = VCCT   CALLED NO =     011533355493

        CALLID =      426449
```

univlog Log

Purpose

The univlog log collects messages regarding CIMS with incorrect format for univ-type sources and entities using the univ converter. Entries include the entire CIM.

Reference

- See "Application logs" (p. 10-22) for other files in $LOGDATA.

Examples

The following are examples of univlog messages:

```
(Fri Apr 28 16:45:55 2003 HP-UX:9000/891:io_svun2:ntp UNIVMsg.C:266

ERR002 EVENT 'svun2' invalid msg: ^A

SITE  00  26/09/03 08:19:50   DLLSTXTA03T

4010ss7 FCD Rec   CallBfr: 272    Site 0

  TS-SZ:26/09/03 07:55:38.9  TS-DISP:26/09/03 07:55:47.6  TimDur:00:
  24:02.1

  CD: Ans  CDflags: RB  Op-CD:

  Out Ans    SS7  carrier:0000  IAR-CD:

  PostDD:0.6  SZ->CarrWnk:0.0  SndrTime:0.0  CarrConn:00:24:10.7

  Called: ISUP 6148607182   Calling: ISUP

  UCRTraps

  OPC:244-233-001  DPC:244-233-004  CIC:141

  Fwd Call Ind: 20 00  Calling Party Cat:0a  Nature of Conn Ind:00

  User Svc Info: 80 90 a2 00 00

  Orig Line Info:00  Bkwd Call Ind:54 04  1st Cause Ind:80 90

  Rel Msg Dir: Fwd

  CIC:----- PC:---/---/---   Sig: ISUP:ss7  Mode: sor

  Carr:0000 ST:on             Cad I:0 O:0    DigRecon:---

^C^A

SITE  00  26/09/03 08:22:18   DLLSTXTA03T

.

.

.
```

backup Log

Purpose

The backup logs record weekly backups of application files and databases. They are named backup.*YY*.*MM*.*DD* .log, for example: backup.990527.log

> **Important!** Although backups are of interest chiefly to the operations and maintenance (O&M) persons who backup up the NTP application, it benefits system administrators to check them, since, if files or databases are lost, it is MUCH easier to restore them, rather than to repopulate them from scratch.

Hint: See "Application logs" (p. 10-22) *for other files in $LOGDATA.*

See Appendix C, "Application Backup and Recovery" for information about backup commands.

Monitor BB-GUI Cleanup

Purpose

The cln_bbgui logs record what is removed when old BB-GUI saved searches, table layouts, and user histories are purged from the system.

These logs, in $LOGDATA, are named bbgui.log*n* , where *n* is a number 0-6 corresponding to a day of the week.

You may wish to monitor these logs to ensure that the old records are being removed properly.

See "Application logs" (p. 10-22) for other files in $LOGDATA.

Creation

This log is created when the **cln_bbgui** utility executes nightly from **cron** (see "ntp crontab File" (p. 2-24)).

Message format

The **cln_bbgui** log starts with:

```
Log file for: Wed Aug 9 06:00:14 EDT 2003
```

Then sections of the log indicate the records that have expired and are being removed. The log includes the user who created the record, their permission, and the associated BB-GUI page.

```
The following bbguitable layout records have expired:
my ascreen layout    djd         user        ascreen
1 row deleted
The following bbguisavedsearch records have expired:
cto search           djd         user        ascreen
1 row deleted
```

See "Customize BB-GUI Attributes" (p. 9-7) for information on how your NTP support organization may customize the retention interval for these BB-GUI records.

Corrective Actions

Purpose

If a monitoring procedure in this chapter requires a corrective action not covered elsewhere in this book, we put the corrective action in this section.

Reprocess CDRs

Purpose

For the following conversions, NTP allows you to manually reprocess CDRs that have failed initial processing. Reprocessed CDRs are NOT used for thresholding and alerting. However, they ARE used for summarization. Since CDRs are not used for summarization until they are (re)processed, you will need the procedures in this section to ensure that the summarized data is as complete as possible.

- AXE10
- IPDR
- Lucent Softswitch
- AXE TRADO
- Any consultant -configured installation

When to use

The frequency with which you should reprocess CDRs depends on your requirements for data summarization.

CDR directories

CIMs from each source in a configurable conversion arrive at NTP in batches. When the CIMs are processed, NTP uses the following directories in the source's home directory on NTP, which was created when the source was added to NTP. Each source has its own home directory (see "Add a Source for a Configurable Conversion" (p. 5-42)).

Directory	Description
processed	Any records that can be processed are sent to the source's processed directory under the same name as the original file. This applies to a whole file or selected records. The processed directory is cleaned out periodically by a **cron job** (see "ntp crontab File" (p. 2-24)).
garbage	If a WHOLE FILE cannot be processed, the file is sent to the source's garbage directory. A CIM file may fail processing because it is the wrong file type, it is misnamed, it has the wrong permissions, and so forth. This directory is cleaned out periodically by a **cron job** (see "ntp crontab File" (p. 2-24)).

Directory	Description
error	If NTP cannot process some records in a file it saves the records to the source's error directory under the same name as the original file. Messages for unprocessed CIMS are logged in the incon log (see "incon Log" (p. 10-29)). You can fix the problems that prevented processing, edit the records in the file if necessary, and submit the file for reprocessing (see "Assign or Modify FDC Group and Network Group/Segments for BB-GUI Users" (p. 7-28).

CDR error directories

A CDR file appears in its source's errors directory if any of its records has one of the following problems. If you correct the problems, NTP can successfully reprocess the records in the file.

Problem	Solution
RE. The RE is not defined in the NTP reference data (or missing).	Add the RE to NTP. See "Add an RE" (p. 4-17). Please note that when you add the RE, note its CLLI. You will need it when you select RE's for reprocessing.
FDC. The FDC is not defined in the NTP reference data (or missing).	Define the FDC in NTP. See "Add or modify an FDC" (p. 4-78). Please note that if the FDC was added to your system on a given date, note the date, as it may be useful when you select CDRs for reprocessing.
Event start and end. The start and end times for the event in this record are out of range or missing. An event cannot: • Be older than the CDR retention interval • Have a time stamp later than the current time (invalid)	If the start and end times in the record have problems, the CDR cannot be successfully reprocessed. However, either (or both) can be used to filter CDRs for reprocessing.

Important! For more information see the re, fdc, start_datime, and end_datime fields in the cfim table in Appendix A of the *BB-GUI User's Guide*.

Error filename

The names of files in CDR error directories contain a time stamp. This time stamp indicates when NTP received the file. This time stamp is different from the time stamp of the individual records in the CDR file and different from the UNIX timestamp associated with the file.

The format of the timestamp is *.D*YYJJJ*.S*TTTTT*, where YY is the year, JJJ is the Julian day, and TTTTT is the time in seconds when the file was placed on NTP.

Which CDRs can you reprocess?

You can reprocess any file in a CDR error directory after you have attempted to fix the problems that prevented initial processing (see the problem and solution descriptions in "CDR error directories" (p. 10-43)).

Reprocessing filters

Within a CDR file, only records that match the criteria you specify are reprocessed. Other records are ignored. You first select a source and then filter by the following criteria:

- **RE** — The system reprocesses all records pertaining to this RE in all files.
- **Time stamp in the error filename, as start or end filter**— As a start filter, all files are reprocessed that NTP received at that time or later. As an end filter, all files are reprocessed that NTP received before and including that time.
- **Any combination of RE plus filename (as start or end filter)**
- **All** (no RE or start/end time)— The system reprocesses all CDR error files if you do not specify a filter.

Multiple reprocessing

You can reprocess a CDR file multiple times. NTP processes the records it can, and returns the remainder of the file to the errors directory for subsequent reprocessing.

Deadline for reprocessing

You can reprocess CDRs for the duration of the CDR retention interval.

Fix GeoProbe Problems in incon Log

Overview

NTP can do CDR CIM conversion for ANY switch monitored by GeoProbe. If *GeoProbe* begins monitoring a switch NTP does not know about, conversion fails, and messages similar to this appear in the incon log (see "incon Log" (p. 10-29)):

```
Fri May 12 08:18:02 2002 HP-UX:9000/785:geoprobeintf_inet1:ntp
  GeoprobeParser .C:255
  ERR002 EVENT DPC 00001600 and OPC 002018000 not in
  swarch/pc2clli tables or CLLI not in rearch table.
```

This type message means that NTP attempted to derive the CFIM's RE, or De (or both) from a DPC, or OPC (or both) on a CDR CIM, but could not:

- The CDR's DPC, OPC, or both, was not in any record's Pc field in the Swarch table.
- The Pc field was populated in Swarch, but the matching Clli was not in any record's RE field in the Rearch table.

Corrective action

- *All.* Add missing point codes and CLLIs to the swarch table, and add CLLIs to the rearch table.
- *5ESS.* For *5ESS* switches with multiple point codes, populate the pc2clli table.

Hint: See "Add an RE" (p. 4-17) .

11 Update the gtspec Table

Overview

Purpose

This chapter describes how to update the gtspec (GTT specification) database table. This table allows you to enter new or changed Global Title data so that Network Trouble Patterning software can provide accurate tabulation and identification of trouble spots via the CFIM fields.

Contents

Introduction

Global Title digit strings

Important! If you are unfamiliar with updating the gtspec table, we strongly suggest you contact your NTP support organization before you use this chapter.

Special service calls, such as 800- INWATS data base calls or 900- service calls, have digit strings that do not contain the full routing information needed to route the call to the terminating entity.

Such information must be obtained from a database containing the routing instructions for the particular service type of the call. This type of digit string is called a global title, since the pattern of digits indicates that the call must first be directed to a global lookup location (usually an SCP) rather than to a specific final destination.

Network elements use global title (GT) digit strings to determine where to forward the call next through a process called global title translation (GTT). GTT (and by extension, NTP) distinguishes one type of service call from another by the pattern of digits in the string; this pattern is called the global title pattern. For example, 800- service calls are distinguished by their 800* digit pattern, and 900-service calls are distinguished by their 900* digit pattern.

NTP's role

When NTP receives a CIM with a digit string that is a global title for a network service, it may need perform a similar global title translation to determine the distant entity (De) to which the failed call was headed. NTP tries to match the digit string in the CIM with a known global title pattern to determine the service type, if possible a record base lookup, and from these and other data the De (if it is not specifically provided in the CIM). This information is then used to populate the fields of the CFIM for the message.

To populate the CFIM fields, NTP must be able to recognize global title patterns. Since this routing data is subject to change in the network, NTP must be kept updated so that it can continue to provide accurate tabulation and identification of trouble spots. For this purpose NTP provides a database table called gtspec (GTT specification) where you can enter new or change existing GT data. The following sections describe how to update the gtspec table.

Terms

Terms used in this chapter are:

- *Global title translation (GTT)* — The process of looking up a dialed string in an external database in order to find where to route the call.
- *Global title (GT) digit string* — A dialed digit string that must be sent to the external database for lookup.

- *Global title pattern* — A pattern that identifies a dialed string as GT.

  Example: If you see a dialed string fitting the global title pattern800 NXX XXXX, then you know the string is an IDB- or DSD-based 800 service, which means it is a GT-type digit string,which means it must be sent to an external database to determinewhere to route the call.
- *Service control point (SCP)* — The external database usually used for GTT.

gtspec Table

Overview

The "gtspec Table" (p. A-77) table is used to tell NTP what global title patterns exist.

Records

Each record in the gtspec table defines a global title pattern. This means that each record tells NTP what it needs to know to:

- Recognize that a CFIM's digit string is a global title pattern
- Do a database lookup, to find a value for the CFIM's DE (distant entity) field

Fields

Fields in the gtspec table are shown in the following table. Please note that:

- The pattern, digtype, st, and gk1 fields are used to calculate the service type (ST) and to find the distant entity (De) in the indicated routing database table.
- The fields starting with gk are used when a De lookup in a routing database table (rdb field) is required.
- The two fields starting with ck are used when a De lookup in a customer database table (cdb field) is required.
- All fields must have something in them, even if it is only a dash (–), which means that the value is unknown.

Field	Function	Value
pattern	The global title pattern. Note that no two records can have the same pattern.	Up to 40 digits or characters. *See* "Global Title Patterns" (p. 11-6).
digtype	The type of digits in the pattern.	• called • calling
st	The service type associated with the global title pattern.	• Up to 5 mixed-case printable characters • - This service type must be defined in the type field of the st table.
gk1	The primary global title record key used for searching the database table specified in the rdb field.	Up to 30 digits or characters from the default character set. There must be a GT key specified in this field when a routing database table (rdb field) is specified.

Field	Function	Value
gk2	The secondary global title record key used for searching the routing database table specified in the rdb field, when the primary lookup fails	Up to 30 digits or characters from the default character set. This field can be filled only if gk1 is filled.
gk3	The tertiary global title record key used for searching the routing database table specified in the rdb field, when the secondary lookup fails.	Up to 30 digits or characters from the default character set. This field can be filled only if gk2 is filled
rdb	The routing database table associated with the global title record key pattern specified in the gk1, gk2, or gk3 fields. This field must have a routing database table specified whenever these fields are specified.	• adjroute • scproute • -
ck1	The primary global title record key pattern used for searching the customer database table specified in the cdb field. There must be a GT key specified in this field when a customer database table (cdb field) is specified.	Not applicable
ck2	The secondary global title record key pattern used for searching the customer database table specified in the cdb field, when the primary lookup fails.	Not applicable
cdb	The name of the customer database table to which the ck1 or ck2 fields refer.	• custid • vpnid • -

Global Title Patterns

Purpose

In NTP, you see global title patterns in the first field of records in the gtspec table.

When a CFIM arrives, the application compares the calling number digits with global title pattern in the gtspec table. If NTP finds a match, it then uses that pattern as a reference into an external database, where a lookup is done to find the CFIM's De.

Parts

The following table gives the parts of each global title pattern. Parts and part order differ for each global title pattern.

Part	Example	Purpose
Digit pattern	800	Specifies digits.
Alphanumeric string	XXXX, Z(3)AF	Each character represents one digit from a set of valid digits.
Delimiter	(A dash.)	Improves readability.

Delimiters

A delimiter is either a:

- Space
- Tab
- Dash

Do NOT use delimiters within digit patterns, such as 800. Otherwise, you can use delimiters in global title patterns as follows:

You can...	Examples
Omit delimiters	800XXXXXXX
Use delimiters between digit patterns and alpha-numeric strings	800-XXXXXXX, 800 XXXXXXXX
Use deliminters within alpha-numeric strings	800XXX-XXXX, 800XXX XXXX, 800-XXX-XXXX, 800 XXX XXXX,

Alphanumeric string parts

Alphanumeric strings are built from the following parts:

Part	Represents...	Example
A,F, V, W, X, Z, Y	0 - 9	NPA-XXX, which expands to [2-9][0-9][0-9][0-9][0-9][0-9]
N	2 - 9	
P	0 - 9	
J	(Valid only in the GT record key fields) Value of V divided by 2.	JV
Q	0 - 4	Q
R	5 - 9	R
~ (key field), - (non-key)	Delimiters (no value)	NPA-XXX
[ ] (brackets)	A range of digits you specify.	AF[0-4]Z, which expands to[0-9][0-9][0-4][0-9]
(d)	(Valid only in GT record key fields) The number found in a position in the dialed string.	(3), which represents the third digit in the dialed string.

Pattern example

1Z(3)AF means: take the dialed digits and interpret them as follows:

- 1 is a fixed value of 1 in the first position of the key (such as the 1 in the dialed 1-800...).
- Z, A, and F are whatever their value was in was in the pattern (in the second, fourth and fifth position in the dialed string).
- (3) means the value in the third position in the pattern is the value to substitute in this position in the key.

If a digit string in a CIM had digits 1234, the digit string would match the pattern definition. In the corresponding record key given in this example, those digits would translate as 14312.

Add a record to this table for each service type you want to collect data on, or for each GT pattern that requires a record base lookup for De determination. Without at least one of these two items of data in the record, there is no point in entering it in the specification.

Pattern variation

If a GT pattern represents a subset of a more general GT pattern in which the subset is included, it may be necessary to list each variation of the general pattern in order to set apart the specific subset. There can be no overlap or ambiguity in the patterns listed in the file or the processing of the associated data is guaranteed to be erroneous.

The network remote access VPN service example given in "gtspec Examples" (p. 11-9) illustrates this point: the GT pattern 12X WXY XXXX indicates an SCPRoute record base lookup. A subset of this pattern, the GT pattern 128 WXY NPAZ, also indicates a specific service type (VPN) not applicable to the more general pattern. The following five records must be added to clearly express all the possible patterns associated with this scenario:

- Pattern: 12[0-7]-WXY-AAAA ST: – RDB: scproute
  This pattern matches strings with 12X combinations less than 128.
- Pattern: 128-WXY-[0-1]AAA ST: – RDB: scproute
  This pattern matches strings with 128-WXY combinations with less than N (N=2-9) in the 7th position.
- Pattern: 128-WXY-NPAZ ST: VPN RDB: scproute
  This pattern matches strings with 128-WXY combinations in which the 7th digit is 2-9, the 8th digit is 0-9, the 9th digit is 0-9, and the 10th digit is 0-9. Note that a matching digit string would have to be restricted to 10 characters, since no provision is made in this pattern for more. This is the only one of the patterns in this set with an VPN service type.
- Pattern: 129-WXY-AAAA ST: – RDB: scproute
  This pattern matches strings with 12X combinations greater than 128.
- Pattern: 12Z-WXY-AAAA-A ST: – RDB: scproute
  This pattern matches strings with all 12X combinations containing more than 10 characters. The pattern 128-WXY-NPAZ would be a subset of this, but if the digit string had more than 10 characters it would match this pattern instead and would not be of an VPN service type.

All these five GT patterns have a global title record key pattern that is expressed as 12(3)-WXY. This record key will search the SCPRoute record base as a De lookup for all five cases. The processing is not dependent on the order of the GT patterns in the file; the result will be correct as long as all cases are covered.

gtspec Examples

Overview

This section gives examples of entries in the gtspec table. Examples do NOT necessarily reflect actual global titles and patterns.

INWATS (IDB) 800 service example

The global title pattern that identifies the digit string of IDB- and DSD-based 800 services is:

```
800 NXX XXXX
```

The GT record key pattern for this pattern is 800-NXX-XXXX. The secondary GT record key pattern is 800-NXX.

The gtspec record for this pattern is:

```
# pattern      digtype  st   gk1        gk2      gk3  rdb
```

Emergency 911 service example

The global title pattern that is identifies the digit string of a 911 emergency service call is:

```
911
```

The length is 3 digits. There is no GT record key for this pattern, and there is no table lookup required. The service type is esc (for emergency service call.)

The gtspec record for this pattern is:

```
# pattern  digtype  st  gk1  gk2  gk3  rdb  ck1  ck2  cdb
```

ACCUNET SDS service example

The global title pattern that identifies the digit string of the ACCUNET SDS service is:

```
700 73X XXXX
```

This pattern can be matched by a digit string of length 10 digits. An extra record is needed to redirect longer patterns. The GT record key for this pattern is 700-73X.

The gtspec records for this pattern are:

```
# pattern       digtype  st    gk1          gk2      gk3  rdb
   ck1  ck2 cdb
 700-73X-XXXX   called   asds  700-73X-XXXX 700-73X  -    -  -
```

Network remote access VPSDN service example

The global title pattern that identifies the digit string of the NRA VPSDN service is:

```
128 WXY NPAZ
```

This pattern can be matched by a digit string of length 10 digits. The length is 10 digits. The GT record key for this pattern is 128-WXY.

This example shows the specific VPSDN service pattern record embedded in the records for the more general pattern 12X-XXX-XXXX as described a few pages back. All five records shown here are necessary to delineate both the general and the specific GT patterns without fatal overlap.

```
# pattern          digtype  st    gk1       gk2  gk3 rdb      ck1
   ck2 cdb
12[0-7]-WXY-AAAA   called   -     12(3)-WXY -     -  -  -    -    -
128-WX- [0-1]AAA   called   -     128-WXY   -     -  -  -    -    -
```

Inbound global VPSDN service example

The global title pattern that identifies the digit string of the inbound global VPSDN service is:

```
198 WXY XXXX
```

This pattern can be matched by a digit string of length 10 or more digits. The GT record key for this pattern is 198-WXY. Reporting entities for these kind of calls are 4 ESS switches only.

The gtspec record for this pattern is:

```
# pattern       digtype  st    gk1      gk2  gk3 rdb   ck1  ck2 cdb
  198-WXY-XXXX  called   gsdi  198-WXY  -    -   scpr  -    -   -
```

Adjunct-bound calls example

The global title pattern that identifies the digit string of adjunct-bound calls is:

```
NPA 0XX XXXX
```

This pattern can be matched by a digit string of length 10 or more digits. The GT record key pattern for this pattern is NPA 0XX. The gtspec record for this pattern is:

```
# pattern       digtype  st  gk1      gk2  gk3  rdb      ck1  ck2
   cdb
  NPA-0XX-XXXX  called   nsc NPA-0XX  -    -    adjroute  -    -    -
```

DSD 900 service example

The global title pattern that identifies the digit string of DSD-based 900 services is:

```
900 NXX XXXX
```

The GT record key for this pattern is 900-NXX-XXXX. The secondary GT record key is 900-NXX.The gtspec record for this pattern is:

```
# pattern       digtype  st    gk1           gk2     gk3 rdb
900-NXX-XXXX    called   mult  900-NXX-XXXX  900-NXX - -
```

Killer trunk service example

The global title pattern that identifies the digit string of a specific "killer trunk" service is:

```
123 456 XXXX
```

This pattern can be matched by a digit string of exactly10 digits. There is no GT record key for this pattern. This pattern is a POTS number that does not require a table lookup, but is a unique service on this pattern. The service type is SCS (for special customer services).

The gtspec record for this pattern is shown below. The second record line is included to specify that a digit string containing more than 10 digits (this pattern contains 11) is not an SCS service type.

```
#pattern          digtype st   gk1 gk2 gk3 rdb ck1 ck2 cdb
 123-456-XXXX     called  scs  - - - - - - -
 123-456-XXXX-X   called  scs  - - - - - - -
```

loadgt Command

Purpose

Use the **loadgt** command (NOT the dbedit command) to update the gtspec table.

Important! Unlike **dbedit** , **loadgt** does not have parameters to specify inserts, updates, or deletes. Instead, you copy a complete gtspec table to an input file, edit the input file, and use loadgt to reload the specification in its entirety. For details on how to do this, see "Update the gtspec table" (p. 11-16) .

Syntax

```
loadgt -f inputfile
 [-o outputfile
] [-s separator
]
```

Option	Function
-f *inputfile*	(Required.) Specifies the ASCII input file containing the gtspec records to be loaded. This is a required parameter.
-o *outputfile*	(If omitted, defaults to **gtspec.error** .) Specifies the name of an output file where the command puts bad records or records not loaded.
-s *separator*	(If omitted, defaults to tabs and spaces.) Specifies a field delimiter character.

Example

The following is an example of **loadgt** output. Note that **loadgt** runs **dbedit** as part of its process.

```
Verifying input file using Ôdbedit' (the Ôgtspec' table will
   not be modified)...
*** 77 lines processed ***
    1 comment line
    76 records inserted
dbedit completed successfully.
All the above transactions have been rolled back.
Performing extra validation of patterns and keys...
*** 77 lines processed ***
    1 comment line
    76 record lines
Loading the Ôgtspec' table using Ôdbedit'...
*** 77 lines processed ***
    1 comment line
    76 records inserted
dbedit completed successfully.
loadgt completed successfully.
```

Update the gtspec Table

Caution!

Errors in gtspec can corrupt application output. If you are not a global title patterns expert, consult an expert before you change this table.

When to update

Update the gtspec table when the network changes global title translations, due to:

- Introduction of new services that use database lookup.
- Changes of routing for existing services.

Update the gtspec table

Purpose

Important! Errors in gtspec can corrupt application output. If you are not a global title patterns expert, consult an expert before you change this table.

Update the gtspec table when the network changes global title translations, due to:

- Introduction of new services that use database lookup.
- Changes of routing for existing services.

Procedure

Use this procedure to update the gtspec table. *Hint: You can modify a copy of the gtspec table ahead of time (Step 1 through Step 3), and later install the changed copy (Step 4).*

1 Use **`sui find`** to copy the existing gtspec table into a temp file

Example: Enter

```
sui find so=gtspec delim='" "' > temp
```

'" "' is single-quote, double-quote, space, double-quote, single-quote.

2 Make a backup copy of the temp file and save it in your home directory.

We suggest you name the file gtspec.*mmdd*, where *mmdd* is the date, such as *gtspec.0527*.

3 Use a text editor (such as *vi*) to edit the temp file to update its global title translation patterns.

Reference: See "gtspec Table" (p. 11-4) for gtspec fields. See "Global Title Patterns" (p. 11-6) for global title translation patterns.

4 Implement the changes by using the **`loadg`** command, with the appropriate options, to load the new gtspec table.

Example: Enter

```
loadgt -f temp
```

Reference: See "loadgt Command" (p. 11-13) for how to use **loadgt**. (The **dbedit** command will NOT work.)

5 View the master error log for messages telling you if **loadgt** failed. To do this, you can use a test editor (such as *vi*). The master error log is in the $LOGDATA directory and is named maste###.#### where ###.#### is the julian date plus the military time when the file was first created.

Example: maste.141.0021

If **loadgt** puts an error into the master error file, then:

- The updated gtspec table did NOT load.
- NTP continues to use the original version of the gtspec table UNTIL the system goes down for any reason.
- When the system goes comes down for any reason, it will be unable to start up again, due to the faulty gtspec table. To prevent this from happening, use the next step.

6 In the master error log, did you see any errors pertaining to your running of **loadgt**?

- If NO, you are done.
- If YES, reload the backup copy of the gtspec table you made in Step 2.

  Important! If you lost the last backup copy, use an earlier backup copy. If you have none, use the original backup copy saved from installation. It is at $MODELDIR/data/ref/gtspec.data.

  Example: If the backup copy is named gtspec0527, and if it is in your home directory, cd to your home directory and enter loadgt -f gtspec0527

END OF STEPS

12 Reference Database Synchronization (RDS)

Overview

Purpose

RDS (Reference Database Synchronization — refsynch) duplicates reference data on pairs of Network Trouble Patterning software hosts, so if one host fails or is cut off from CIMs, users can log on the other host.

Contents

Description

Two groups of data

Recall that data can be classified into two groups:

- *Reference data*. Data defining the customer network.
- *Surveillance data*. Data from REs, and data created from that data (such as cim, acase, alert, cfim, fdccount, otr, and linkalert tables).

This illustration shows how RDS works in relation to these data types.

What data is synchronized for RDS?

RDS synchronizes reference database tables on two hosts. The list of tables synchronized for your system is in the bdrsynclist table. (This is an internal table that only your NTP support organization can modify if needed.) Tables that can not be synchronized are:

- Reference database table: source, cmdlog, err2bsyncd, fdc_audit, indkdial, enutables, outdkdial, samplingrate, sysuser, trapalert, sysuser, event_status.
- Surveillance data tables. These tables are not synchronized but should be similar if the two hosts have identical data feeds. Some minor variations may occur because of application down time, thresholding differences, etc.

  Important! Synchronized tables are analyzed by the **`bdr_syncref`** and **`bdr_auditref`** commands (see "bdr_syncref" (p. 12-10) and "bdr_auditref" (p. 12-11)).

Connections for RDS

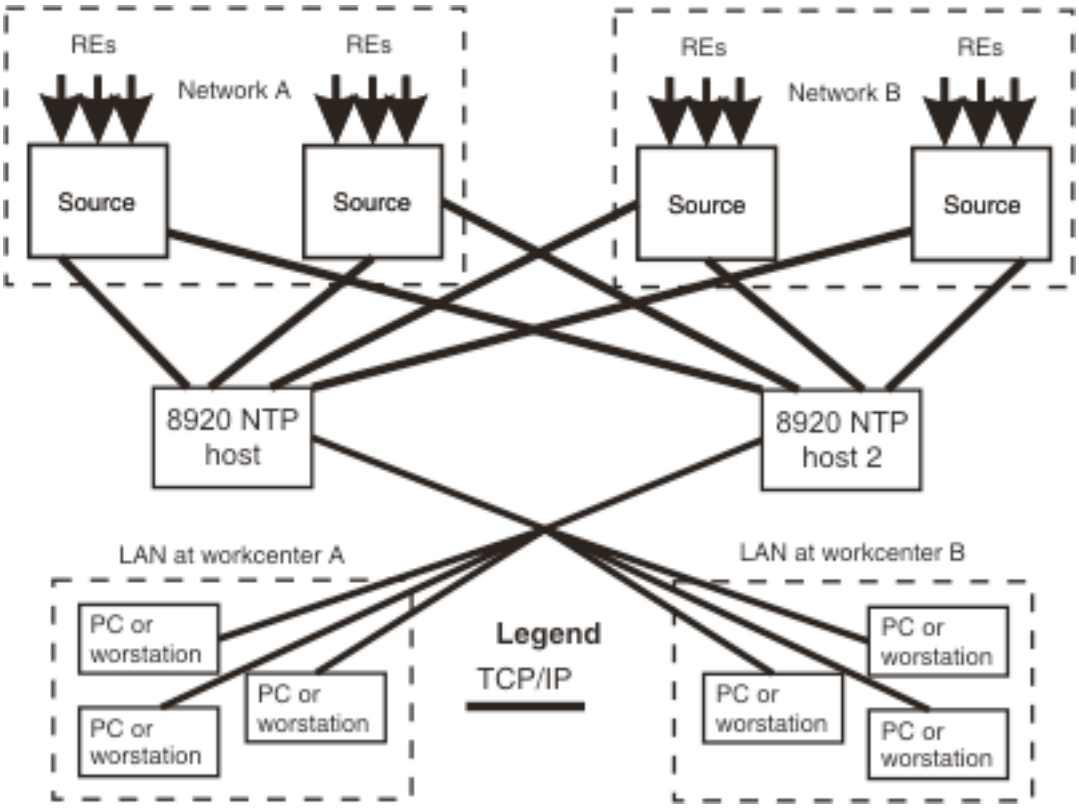
Description

Before RDS can be installed on your system, the following has to be done to establish connections.

Task	Who does	Note
Set up TCP/IP between pairs of NTP hosts.	You and TCP/IP administrator	See your TCP/IP administrator and Chapter 5, "CIM Source Administration".
Set up duplicate CIM feeds from each source to NTP host pairs.	You and source administrator	For NFM sources, also see Appendix D, "Set Up 8925 Integrated Service Assurance". For CP sources see *CP Administration and O&M*.

Connections for RDS

This example shows connections among components involved with RDS.



Important! 4E offices which connect to one and only one CP. The CP forwards data to both Hosts. A CP source may reside on its NTP host. Data is routed similarly.

Monitor Synchronization

RDS task overview

To maintain reference database synchronization, you must monitor systems messages as they arise, and well as do routine checks. The following tables tell what to do.

- "Check often for RDS" (p. 12-4)
- "Check occasionally for RDS" (p. 12-5)

Check often for RDS

Check the following often:

Check	When	What to do	Reference
Did **bdr_syncref** put a completeion message in the *bdrlog.juliandate*?	Each morn-ing	if the command was successful, no action is needed. If the *bdr* log indicates that some records were unsuccessful, look in the *err2bsyncd* table to see the differences and use the **bdr_syncerr** command to attempt a resynchronization. Use **bdr_auditref** to compare the two tables.	• "bdr_syncref" (p. 12-10) • "Monitor Application Logs ($LOGDATA)" (p. 10-22) • "dbedit Command" (p. 3-22)
Did **bdr_syncref** put a message in *$LOGDATA/bdrlog* `julian_date` saying the command failed?		You missed a day's update. Run **bdr_syncref** manually.	• "bdr_syncref" (p. 12-10) . • "Monitor Application Logs ($LOGDATA)" (p. 10-22) • "master Log" (p. 10-25)

Check occasionally for RDS

Check the following occasionally or when troubleshooting RDS.

Check	Reference
Cron . Ensure that the ntp crontab file has entries for: • **bdr_syncref** —default daily at 00:30 • **bdr_cleanup** — default daily at 02:30	Sections in "ntp crontab File" (p. 2-24)
Dual user logins . When adding or deleting user logins, ensure that each user has identical logins on both NTP hosts in a host pair.	• "Add an NTP user" (p. 6-22) • "Delete an NTP user" (p. 6-30)
Tables . Ensure that the correct tables are being synchronized.	"What data is synchronized for RDS?" (p. 12-2)

Configure RDS feature

Purpose

The RDS feature requires proper configuration before it starts operation. The procedure included in this section shows how to configure it.

Important! Please consult your Alcatel-Lucent customer engineer prior to performing this configuration.

Before you begin

Important! Each step of this procedure needs to be performed on both host machines. For the example outputs below we will refer to "hosts" as **host_a** and **host_b**.

You will need the following information to complete certain steps:

- the remote host's IP address and machine name to make the **/etc/hosts/** file entry
- the IP addresses and machine names of all sources that will connect to each host to populate the **/etc/hosts** files.

Procedure

Use this procedure to complete configuration of the RDS feature:

1 Log on the 8920 NTP host as **root**.

2 Populate the **/etc/hosts** file to allow communications with the other 8920 NTP host and all workstations (servers) that will access 8920 NTP.

Reference: "Host TCP/IP Administration" (p. 5-14)

3 Set up Oracle **tnsnames.ora**.

Important! The proper way is to make the names unique in the **tnsnames.ora** file (for example, use **<remote machine>.world** for the remote machine). If the **ntp.world** is used for both the local and the remote machine, it will cause installation problems.

Use a text editor (such as **vi**) to edit the **/etc/tnsnames.ora** file to add the connect description of the remote host destination.

- Enter **vi /etc/tnsnames.ora**
  Important! The **dbms.world** entry should exist on both hosts.
  Example:

This is an example of the entries for each host in the **tnsnames.ora** file. This should be performed on each host.

```
host_a.world =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS =
(COMMUNITY = ntp.world)
(PROTOCOL = TCP)
(Host = host_a)
(Port = 1521)
)
)
(CONNECT_DATA = (SID = dbms)
)
)
host_b.world =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS =
(COMMUNITY = ntp.world)
(PROTOCOL = TCP)
(Host = host_b)
(Port = 1521)
)
)
(CONNECT_DATA = (SID = dbms)
)
)
```

- Enter: **vi $TNS_ADMIN/listener.ora** and add the SID entry (may have already been done).

  Example:

  This is an example of the changes to the **listener.ora** file, including the SID entry.

```
SID_LIST_LISTENER =
(SID_LIST =
(SID_DESC =
(SID_NAME = dbms)
(ORACLE_HOME = /lucent/ntp/oracle)
(PRESPAWN_MAX=5)
)
)
```

Note:

- No changes to the **sqlnet.ora** file should be necessary on either host.
- No other functions are necessary, if the **tnsnames.ora** file is modified.
- Stop and restart the Oracle listener processes on both hosts: **lsnrctl stop**; **lsnrctl start**.

4 Set up the host-to-host database link on each host.

1. Login as **ntp** on **host_a**.
2. Use **opwd db$** on host_b to get the db$ passwd.
3. Execute the **create_link** command.

Syntax:

create_link <db$_passwd> <remote_host>

Perform the same operation on host_b.

If the create_link command is successful, it will print the name of the remote host.

5 Logged in as **ntp**, execute **$SNASDIR/appl/etc/reftrig disable** to disable the RDS triggers.

You can run the following command in sqlplus to get the current status of RDS triggers:

"select trigger_name, status from sys.dba_triggers where trigger_name like '%_REF_%';".

6 Contact your Alcatel-Lucent Customer Engineer to enable the Reference Database Synchronization feature.

END OF STEPS

Commands Overview

Hosts and command syntax — local and remote

The syntax of RDS commands refers to a pair of NTP hosts as local and remote. Either host can be local or remote, depending on where you run the command:

- **`Local`** — The NTP host where you run the command
- **`Remote`** — The other NTP host

RDS command summary

The following commands are used to maintain or check RDS.

Important! **`ntp crontab`**. By default, all but the **`bdr_auditref`** command are run from the ntp crontab file. See "ntp crontab File" (p. 2-24) for more information.

Command	Run from crontab?	Run on both hosts?	Purpose
`bdr_syncref`	Yes, daily at 00:30 (default)	Yes	Gets reference data changes from the remote NTP host and puts them on the local host.
`bdr_syncerr`	It does not run from crontab.	Yes, runs on both hosts.	**Bdr_syncerr** tries to resynch on the local host any records that failed during a previous execution of bdr_syncref. The user can use sui find to examine the err2bsyncd table to see what records err2bsyncd will attempt to resync.
`bdr_cleanup`	Yes, daily at 23:30 (default)	Yes	Removes any records from the local rec2bsyncd table that have already been synchronized on the remote host.
`bdr_auditref`	No, use only for troubleshooting.	No. Only one host needs to run it.	Compares reference data between NTP hosts. By default, it compares the number of records in every active table in *bdrsynclist*. Given a table *name* argument, it creates two difference tables on the local host. These difference tables can be used to create **dbedit** files to manually synchronize the tables (see "dbedit Command" (p. 3-22)) to manually synchronize the local host.

bdr_syncref

Purpose

The **bdr_syncref** command synchronizes reference data tables between two NTP hosts (see "What data is synchronized for RDS?" (p. 12-2)).

When to use

Run the command:

- Daily, automatically from ntp crontab on BOTH NTP hosts (see"ntp crontab File" (p. 2-24) for a crontab example). Default is 00:30.
- Manually, if a message in $LOGDATA/bdrlog*julian_date* tells you **bdr_syncref** failed when run from crontab.

  Important! Once it runs successfully, if you try to execute **bdr_syncref** a second time in the same day, it will fail (until the **bdr_cleanup** command runs from cron at 11:30 p.m.).

Syntax

```
bdr_syncref
```

Response and output

If you run from command line you'll see messages. If run from crontab, messages go to *bdr_log* only.

- **bdr_syncref** success or failure is logged in the $LOGDATA/bdr_log file (see "Monitor Application Logs ($LOGDATA)" (p. 10-22) for how to read log files).
- **bdr_syncref** fails if the hosts cannot communicate, or if NTP is down on either host.

Output includes:

- the number of records retrieved from the remote host,
- the number of records updated, inserted or deleted on the local host,
- the number of records that failed synchronization on the local host,
- and the date and time synchronization completed.

bdr_auditref

Purpose

The **bdr_auditref** command reports discrepancies between reference database tables on two NTP hosts. It checks the same tables flagged for **bdr_syncref** synchronization. See "What data is synchronized for RDS?" (p. 12-2) for the list of tables.

When to use

Run **bdr_auditref** on either of the NTP hosts when troubleshooting. Remember that changes you make to either host's reference data show up as discrepancies until they are synchronized by **bdr_syncref** at 23:30.

Syntax

By default, **bdr_auditref** compares the number of records in each active table in *bdrsynclist*. Any discrepancies will be printed to stdout. The number of records in the err2bsyncd table is also printed to stdout

```
bdr_auditref [-t tablename]
```

Parameter	Description
-t tablename	This optional parameter, followed by a table name, specifies a single table to audit. Omit this to audit ALL synchronized reference tables.

Response and output

In the default case, **bdr_auditref** all active tables in the *bdrsynclist* table and prints the table name, the number of records in the local table and the number of records in the remote table for every table with a record count discrepancy.

If a single table is audited, the command creates two new tables called <*table*>_*loc* and <*table*>_*rem* and prints the number of records in each table. The user can use the **sui find** command to examine the contents of these tables. Records that appear only in the <*table*>_*loc* table are missing from the remote table. Records that appear only in the <*table*>_*rem* table are missing from the local table. Records that appear in both the <*table*>_*loc* and <*table*>_*rem* tables exists on both hosts but have some differences.

Running the **bdr_auditref** command on the same table on the remote host will result in an _loc and _rem table that will be the opposite of the _loc and _rem tables on the local hosts.

Manually correcting discrepancies found by bdr_auditref

Purpose

Discrepancies found by the **bdr_auditref** command are saved in ASCII files which can be used for updating the databases. Care should be taken when manually correcting records or errors will result.

Procedure

Use the following steps when manually correcting discrepancies.

1 Determine what records from the <*table*>*_rem* table need to be updated on the local host

2 Create a **dbedit** file on the local host using the **sui find** command, for reference see "ASCII Files for dbedit" (p. 3-20).

```
sui find so=<table>_rem delim=\| nohead > <table>.db
```

3 Enter

```
reftrig disable
```

Note: Any changes made while the RDS triggers are disabled will not be saved for later synchronization.

4 Use the **dbedit** command to make the desired changes to the local table, for reference see "dbedit Command" (p. 3-22).

```
dbedit -iu -t <table> -f <table>.db -s \|
```

5 Enter

```
reftrig enable
```

Note: Any changes now made to the reference data will be saved for later synchronization.

6 Enter

```
bdr_auditref -t <table>
```

to see if **dbedit** synchronized the table.

END OF STEPS

bdr_cleanup

Purpose

The **bdr_cleanup** command deletes records from the local *rec2bsyncd* table that have already been synchronized on the remote host.

When to use

Run **bdr_cleanup** from crontab daily on BOTH hosts (see "ntp crontab File" (p. 2-24)for a crontab example). Default is 23:30.

Syntax

```
bdr_cleanup
```

There are no arguments or options for this command.

Response and output

The last synchronization date retrieved from the remote host and the number of records deleted from *rec2bsyncd* are written to the bdr log. If **bdr_cleanup** is run from the command line, these messages are printed to *stdout* also.

13 Configurable Summarizers

Overview

Purpose

Summarizers are used by NTP to gather data from specified fields within a CFIM. NTP comes with a standard set of summarizers and summary tables. The Configurable Summarizer feature allows the System Administrator to build custom summarizers/summary tables that can report on any field or set of fields in the CFIM that are user-viewable.

Contents

Overview of Configurable Summarizer Feature

Purpose

This feature provides command-line tools that enable a NTP system administrator to design, implement, and manage new summary tables and summarizers. These user-built summary tables have the flexibility to report on any field or set of fields in the CFIM that are user-viewable.

After collecting this information from the user, the tool will create a new summary table which is viewable by the BBGUI, using Find and Compute.

cs_admin table

The **`cs_admin`** table is a user-viewable reference table used in the administration of the Configurable Summarizer feature. The NTP user can populate it with **`cs_create`** and **`cs_stat`** commands.

Limitations

The tool has the following limitations:

- There is a maximum of 10 active custom summarizers.
- There is a maximum of 1000 rows per summarizer per hour.
- The data is summarized at the hour level (i.e., the summary data will have a granularity of one hour).
- Only two filters are allowed (i.e., additions to the where clause).

Examples

Following are two examples of custom summarizers.

To create a summarizer and a summary table that contains the hourly count and sum of duration of successful 800 calls, use the following:

SUMMARY_TABLE_NAME	CONDITIONS	CFIM_FIELDS
CompleteCallsTo800	fdc='comp' and digits=800*	cnt, sum(durat)

To create a summarizer and a summary table that contains the count and duration of long duration calls to India, use the following:

SUMMARY_TABLE_NAME	CONDITIONS	CFIM_FIELDS
IndiaSuspectCalls	ccd=91 and durat>100	cnt, sum(durat)

Create a Configurable Summarizer

Purpose

The Configurable Summarizer Create (**cs_create**) command:

- builds and tests new scripts,
- builds a new summarizer table – including all usual helptext,
- populates all necessary administrative tables.

Important! Summarizer additions and deletions do not take effect until the **ntpstop** and **ntpstart** commands are run.

Command Syntax

cs_create [-?]

where: **[-?]** provides usage information

Specifying fields of the selected table

Any one summarizer can have up to 5 calculated fields from the selected table. Calculations are limited to summing fields (sum()) and counting (count(*)).

The following fields are automatically included in the summarizer:

- datime
- date
- time
- count (results of count)

Refer to *BB-GUI User's Guide*, Appendix A, "Surveillance and Summary Database Tables", for detailed information about the CFIM Table and the fields associated with it.

Specifying Search Expressions

The **cs_create** command prompts you for a search expression. A search expression is a set of criteria that limits output. Search expressions in **cs_create** can be specified using a subset of those available with the **sui find** command. Those expressions are:

- none
- =
- !=
- -
- *
- <
- >

Refer to *System Administration Guide*, Chapter 4, "Reference Database Tables", the section "Search Expressions in sui Find" for detailed information about use of these search expressions.

Procedure

Important! User is able to exit or abort *cs_create* at any prompt by typing '**quit**'.

Use the following procedure to create a summarizer.

1 Enter

cs_create

Result: You are prompted for a summarizer name.

2 Enter the name of the summarizer/table you wish to store the results in.

Result: You are asked if you want this summarizer to be active.

3 Enter **y** to make the summarizer active

Enter **n** to create the summarizer, but leave it inactive.

Important! There can be no more than 10 active summarizers.

Result: You are prompted to enter a name of Source Table.

4 When you have entered the name of Source Table, you are prompted for up to 5 source fields, operators, values, and Destination fields.

If you have fewer then 5 source fields, enter a value of . (period) to end the prompting and move to the next step.

Result: You are prompted to enter a number of Retention Days.

5 Enter the number of days of data you wish to keep in the summary table. The default is 366 days and the maximum is 999 days. After reaching the specified retention day number, the oldest rows will roll off.

Result: You are prompted to enter a Start Date.

6 Enter a start date to specify how far back in the CFIM table this will begin. The default is the current date. The earliest allowable date is that of the oldest record in the CFIM table.

Result: You are prompted to enter an End Date.

7 Enter an end date to deactivate the summarizer. The default is 60 days from the current date.

Result: The data you have entered is presented to you for verification.

8 If you would like to edit the information, enter n and make any necessary changes.

If the information is correct, enter **y**.

Result: You are prompted to enter a **Frequency choice**.

9 Enter a frequency choice ('h' - indicates the summarizer is run hourly and 'd' indicates it is run daily). The default is 'h'.

Result: you are prompted to enter a description of the summarizer.

10 Enter descriptive information about the summarizer, as desired. Up to 255 characters can be entered.

Important! Summarizer additions do not take effect until the**ntpstart**commands are run.

Result: The tool completes the summarizer creation process and returns a success message.

END OF STEPS

Example

The following example creates an active summarizer/table named non-comps containing the source fields re, de, and fdc. The data runs for two months and is retained for 100 days.

```
>cs_create
Custom Summarizer Creation.
You will be prompted for several data items.
You can select up to 5 fields from the cfim table.
You can also select summations on fields such as SUM(durat) but at
   least one of the fields must come directly from the source table
   without being summed.
COUNT(*) is always included for you.
You may abort at any time by typing 'quit'.
Summarizer Name> non_comps
```

```
Active(y/n default=y)> y
You will be prompted for up to 5 database fields
If you have fewer then that, type a '.' to break out
Source Field1> re
Operator1(=,!=,<,> default=none)>

Destination Field1(default=re)> re_dest
Source Field2> de
Operator2(=,!=,<,> default=none)>

Destination Field2(default=de)> de_dest
Source Field3> fdc
Operator3(=,!=,<,> default=none)> !=
Value3> comp
Destination Field3(default=fdc)>

Source Field4> .
Retention Days(default=366) > 100
Start Date(default=05/23/2005) >

End Date(default=07/23/2005) >

You are creating a new summarizer named non_comps
With the following actions:
SELECT re FROM cfim INTO re_dest
SELECT de FROM cfim INTO de_dest
SELECT fdc FROM cfim WHERE != 'comp' INTO fdc
Data will be retained in this table for at least 100 days.
Data will start accumulating on 05/23/2005 and will stop on 07/23/2005.
Continue with summarizer creation(y/n)? y
Updating administrative tables....
1 row created.
Testing new summarizer.....
Creating test table....
Creating test summarizer....
Testing test summarizer....
Removing test table....
The new summarizer is ok
Building new table and summarizer...
Creating new table...
Creating new summarizer...
Updating shared memory...
A new summarizer and table named non_comps and a new script named non_
   comps.cfim were succesfully created.
```

View Configurable Summarizer Status

Purpose

The Configurable Summarizer Status (**cs_stat**) command is used to:

- view custom configured summarizers and the alert notifications that depend on those summarizers
- activate and deactivate summarizers
- change summarizer start/end date
- change number of retention days.

Command Syntax

```
cs_stat [-?] [ -s <summarizer_name
> [ -act|-deact ] [ -oldest
   ] [ -newest ] [ -start_date MM/DD/YYYY ] [ -end_date
   MM/DD/YYYY ][ -retention NNN ] ]
```

Options are as follows:

Option	Description
[-?]	Provides usage information and exits.
-s <summarizer_name>	Restricts the specified actions to this particular summarizer.
[-act|-deact]	(Optional) Activates or deactivates the specified summarizer.
[-oldest]	(Optional) Displays the date of oldest valid data for the specified summarizer.
[-newest]	(Optional) Displays the date of newest valid data for the specified summarizer.
[-start_date MM/DD/YYYY]	(Optional) Changes the summarizer start date to MM/DD/YYYY. This field can also be set to NULL (i.e., a blank entry or <*space*>), which instructs the summarizer to use the earliest possible start date.
[-end_date MM/DD/YYYY]	(Optional) Changes the summarizer end date to MM/DD/YYYY. This field can also be set to NULL (i.e., a blank entry or <*space*>), which instructs the summarizer to run with no specified end date.
[-retention NNN]]	(Optional) Changes the retention days to NNN.

Examples

The following examples illustrates some of the various uses of the **cs_stat** command.

Example 1

This example shows output for the **cs_stat** command with no options specified.

>cs_stat

```
Summarizer Status from the cs_admin table:
Summarizer Active Start    End      Retention
foo           y   05/22/05 05/22/2006 5
foobar        y   03/05/05 07/23/2005 100
gcn           y   05/22/05 05/22/2006 366
jmb8          y   04/23/05          366
non_comps     y   05/01/05 05/22/2006 100

Alert_notifications that depend on the configurable
  summarizers:
Alertname      Summarizer
foo                foo
foobar             foobar
```

Example 2

This example shows use of the **cs_stat** command to deactivate the non_comps summarizer.

>cs_stat -s non_comps -deact

```
The deactivation of summarizer non_comps succeeded.
```

Example 3

This example shows use of the **cs_stat** command to change the start date on summarizer jmb10 to 07/01/2005.

>cs_stat -s jmb10 -start_date 07/01/2005

```
The date for summarizer jmb10 was successfully updated to 07/01/2005
```

Example 4

This example shows use of the **cs_stat** command to change the end date on summarizer jmb10 to 08/01/2005.

>cs_stat -s jmb10 -end_date 08/01/2005

```
The date for summarizer jmb10 was successfully updated to 08/01/2005
```

Example 5

This example shows use of the **cs_stat** command to change the end date on summarizer jmb10 to NULL.

```
>cs_stat -s jmb10 -end_date
```

```
The date for summarizer jmb10 was successfully updated to NULL
```

Example 6

This example shows use of the **cs_stat** command to change the number of days the data is retained for summarizer jmb10 to 400.

```
sf44016.ntp% cs_stat -s jmb10 -retention 400
```

```
The retention time for summarizer jmb10 was successfully updated to 400 days
```

Delete a Configurable Summarizer

Purpose

The Configurable Summarizer Delete (**cs_delete**) command is used to delete summarizers and tables.

Important! Summarizer additions/deletions will not take effect until the next ntpstop/ntpstart cycle.

Command Syntax

cs_delete [-?] [-s <*summarizer_name*>]

Options are as follows:

Option	Description
[-?]	Provides usage information and exits.
[-s]	*<summarizer_name>* is the name of a summarizer in a diactivated state.

Procedure

Use the following procedure to delete a summarizer.

1 Enter

cs_delete -s <*summarizer_name*>

Result: You are asked to confirm that you want to delete this summarizer.

2 Enter **y** to delete the summarizer.

Enter **n** to exit the tool.

3 When you have entered **y** to delete the summarizer, the tool completes the deletion process and returns a success message.

Important! Summarizer deletions do not take effect until the **ntpstop** and **ntpstart** commands are run.

END OF STEPS

Example

Enter

cs_delete -s non_comps

```
Deleting summarizer script and data for non_comps, OK(y/n)? y
Deleting model table...
Deleting data table...
Summarizer non_comps was successfully deleted.
```

Appendix A: Reference Database Tables

Overview

Purpose

This appendix describes the user-modifiable database tables that hold Network Trouble Patterning software reference data. These tables are used to parse, interpret, and manipulate Surveillance, Summary, and Periodic data information.

Contents

Introduction

Overview

Reference database tables are user-modifiable tables used to parse, interpret, and manipulate data in the Surveillance, Summary, and Periodic database tables.

Multiple types of tables

In addition to Reference database tables, there are other types of tables used by NTP.

- *Surveillance data tables* — These tables are populated in real time as a result of input data streams from CIMs. This information is used to populate NTP outputs such as Alert Cases, TrapAlerts, and other displays on the BB-GUI. These tables are not modifiable. Surveillance database tables are sometimes referred to as *chronological* tables.

  Reference: Surveillance database tables are detailed in Appendix A, "Surveillance and Summary Database Tables", in the *BB-GUI User's Guide*.
- *Summary data tables* — these tables contain calculated information used in reports.

  Reference: Summary database tables are detailed in Appendix A, "Surveillance and Summary Database Tables", in the *BB-GUI User's Guide*.
- *Periodic data tables* — these tables contain information that is collected periodically, such as every 15 min. or 1 hour. Periodic tables cannot be modified.

Internal ("hidden") tables

NTP has many tables that are modified by internal processes but that are seldom, if ever, manually modified. You may have occasion to view data in internal tables (with the **`sui find`** command), but you do not modify them. For example, in procedures to monitor links, you may view the internal linkstatus table. This appendix does NOT describe internal tables.

Reference: See “menutables Table” (p. A-104) for more information on how to tell if a table is internal or user-modifiable.

Accessing Table Descriptions

Overview

Reference database tables are listed in this Appendix. The listings contain general information about the tables as well as special notes and dependencies.

Generally, the following information is presented for each table:

- Purpose — a description of the table.
- Field Dependencies — a listing of fields in other tables that must be populated or must match a particular field in this table.
- Special Considerations/Notes — information to be aware of when working with this table.
- Example — if necessary.
- Reference — if necessary.

Field Information

The listings in this appendix do NOT contain a listing of the fields within these database tables. Because the fields in these tables change frequently and are highly dependent on the options and features enabled on your NTP system, the most accurate information is available on the NTP software itself. See "Viewing Table and Field Descriptions" (p. A-8).

Important! NTP translates all field names and values to lowercase unless there is a specific constraint on a field within the system. In those few instances, the value appears in case-sensitive format. For example, for ease of reading, the Description field retains a mix of upper- and lowercase letters.

Modifying Reference Database Tables

Please refer to Chapter 3, "Reference Data Tables" for detailed information on how to modify Reference database tables.

Viewing the tables

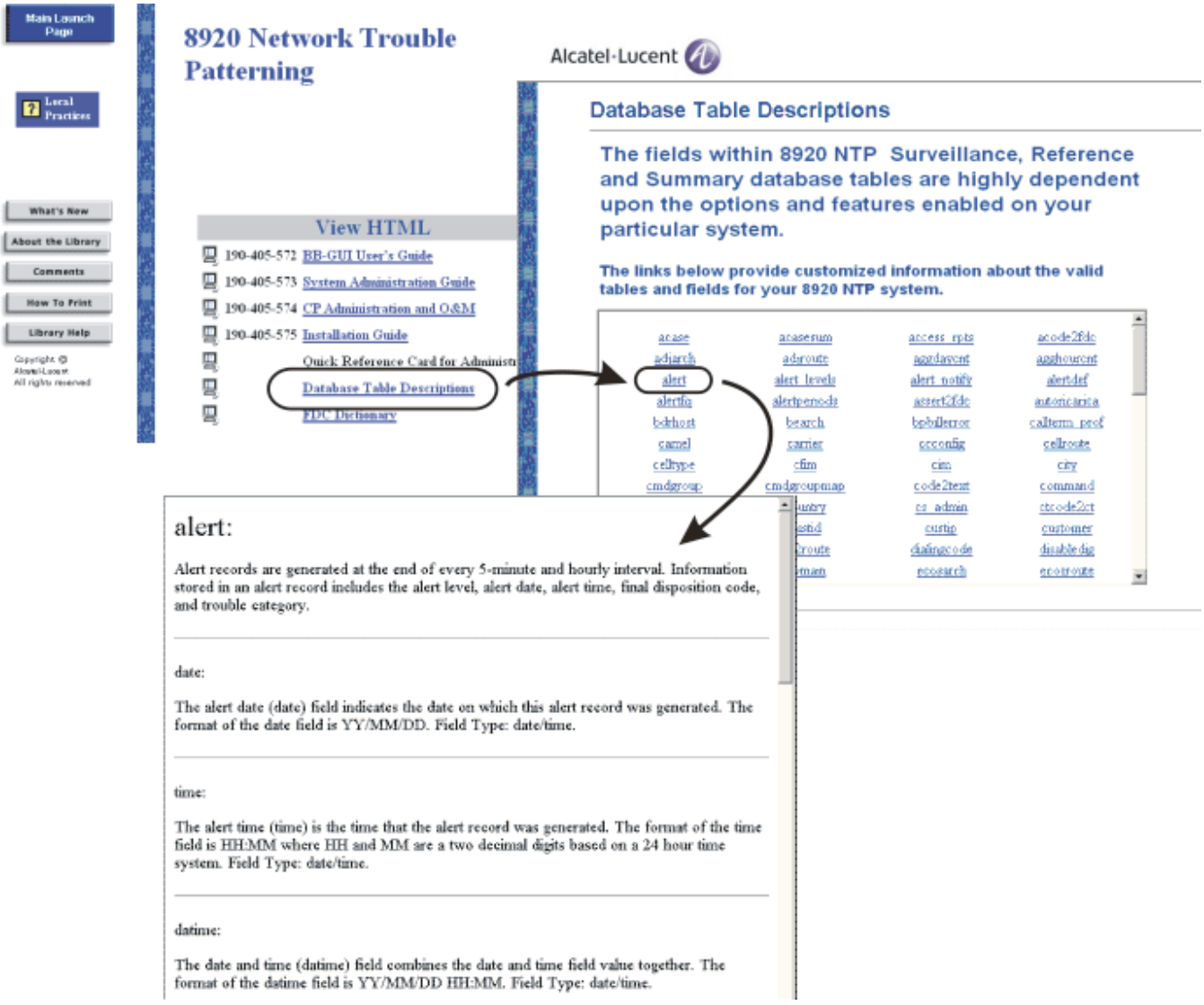
To see records in any table except Trapalert, use the Find Page, detailed in Chapter 5, "Analyze" in the *BB-GUI User's Guide*.

On any page (e.g., Find Page), column help is accessed by right-clicking on an output column and selecting "column help".

Viewing Table and Field Descriptions

There are two ways to view descriptions of tables and their associated fields:

- The **`describe`** command, which is accessed from the command line (administrators only). This command is described in detail in the section "describe Command" (p. 3-10).
- The Database Table Description link, which is accessed from the Library Page. This link presents you with a listing of all tables found on your system. Select a table and you are presented with output detailing the valid fields for the selected table.



acode2fdc Table

Purpose

Used if RE is as follows.

If a CIM is from conversion	Acode value is in CIM's	Fname value is in CIM's
1AESS	NA. (Use "ess1a2fdc Table" (p. A-63) .)	
4ESS	NA. (Use the CIM's FHC code.)	
5ESS MDII's	NA.	
Alcatel 5020 Spatial Softswitch		alcatelss
AUTOPLEX MSC	failure reason text	
EVDO CP Fail	failure reason text	evdo_cpfail
EVDO PCMD	failure reason text	evdo_pcmd
PCMD	failure reason text	the log name
Ericsson SGSN		Ericsson_SGSN
DMS MTX MSC	failure reason text	the log name
OTR		
DMS	See "Special considerations" (p. A-10)	
EWSD	caus	
S1240		
Succession SN05 and SN06		
GeoProbe	See	
AXE 10		Always "billdats"
AXE 10 TRADO		
Lucent Softswitch		
NGSS	sip/siplog	4xx, 5xx or the log name
SDHLR OM	message ID	sdhlr_om
GPRS	message ID, ccittQ767Cause: *[value]*	S-CDR
	message ID, gsm0408Cause: *[value]*	M-CDR
	gsm0902MapErrorValue: *[value]* , gsm0408Cause: *[value]*	S-SMO-CDR

If a CIM is from conversion	Acode value is in CIM's	Fname value is in CIM's
Nortel GSM	failure reason text	ncdr_<xxx>

The "actual code to FDC" (acode2fdc) table contains a fdc translations. A tilde, "~", in any key field means "don't care" or match anything.

Example: A DMS message with a single message name (for example, LINE138, TRK113, C7UP123, or TCAP101) can represent many different call failure or event types. Detailed call event data is contained in the message'sreason/trouble code, which can be up to 80 characters in length and can be used to represent different problems in different CIMs.

To uniquely identify an SCP, DMS or 5ESS DSE CIM as a specific FDC on which NTP can perform counts, thresholding, and alerting, each message name must be associated with each reason/trouble code or treatment set and assigned an FDC identifier. You must therefore build a record for each message name/reason code combination, and give each combination an FDC. FDCs must be defined in the fdc table before they can be used here.

Reference: See Step 13 in "Add or modify an FDC" (p. 4-78) for when this table is used.

Field dependencies

In table...	Before you put a value in field...	That value must be in field...	In table...
acode2fdc	fdc	fdc	fdc

Special considerations

- `DMS 100, 200, 250, and 500 Messages`

  DMS switches send messages with a single message names (such as: LINE138, TRK113, C7UP123, or TCAP101) which can represent many different call failure types. Detailed call failure data is contained in the message's reason/trouble code which can be used to represent different problems in different CIMS. In TRK and LINE messages, these codes are named with the keywords:

  – TRBCOD:
  – TRBCODE:
  – TRBCODE=
  – TROUBLE=
  – TROUBLE CODE:
  – TROUBLE CODE=
  – TREATMENT SET

In acode2fdc records, these keynames map to the fname field. The actual trouble code or treatment set maps to the acode field. Some trouble/reason codes contain a variable (usually numeric) at the end of the text, as in "OUTAGE ON CARR n". Since the NTP CFIM converter reads Acodes on a "best match" basis, it is not necessary to include the variable in acode strings. The acode string OUTAGE ON CARR will match all occurrences of this reason code and find the appropriate FDC.

- `DMS AUDT Messages`

  AUDT is a type of DMS log message. Currently two types of AUDT logs are supported:

  – *AUDT105* - Trunk Reset - when there is an incorrect trunk state and the system recovers the trunk.

    The following template is used for AUDT105:

    ```
    AUDT105 a  INFO TRUNK RESET
    TRUNK b  CALLID c
    FROM STATE d  TO STATE e
    ```

    where:

    a: timestamp (format: mmmdd hh:mm:ss ssdd)

    b: trk id

    c: call id

    d: initial trunk state description

    e: final trunk state description

    An example of an AUDT105 log message is as follows:

    ```
    AUDT105 APR01 12:00:00 2112 INFO TRUNK RESET
    TRUNK CKT HSTNTX0144TO 7280 CALLID 690122
    FROM STATE CPB TO STATE IDL
    ```

  – *AUDT106* - Trunk Force Release - a call is forced down by the release of a trunk.

    The following template is used for AUDT106:

    ```
    AUDT106 a  INFO TRUNK FORCE RELEASE
    TRUNK b  CALLID c
    ```

    where:

    a: timestamp (format: mmmdd hh:mm:ss ssdd)

    b: trk id

    c: call id

    An example of an AUDT105 log message is as follows:

    ```
    AUDT106 APR01 12:00:00 2112 INFO TRUNK FORCE RELEASE
    TRUNK CKT HSTNTX0144TO 7280 CALLID 46372
    ```

- `DMS DFIL Messages` DFIL (Data Fill) is a type of DMS log message. Unlike DMS TRK and LINE messages (mentioned above), DFIL messages do not contain a trouble code or keyword. Instead, they contain a DFIL number (the string "DFIL" with a 3 digit numeric code) and the date and time of the log.

  An example of a DFIL100 log message is as follows:

  ```
  *DFIL100 JAN01 09:21:03 XXXX FAIL TRANSLATION ERROR HOST 00 1
   04 19 DN 9097224112 OG CKT = TOPOGNY 1, CALLED DR =
  ```

90114466062112345 PREFIX DR = $, SUFFIX DR =
0114466062112345 MORE THAN 15 DIGITS IN 1 STAGE OF OUTPULSING
Most DFIL message numbers are contained in the acode2fdc table by default and are mapped to an appropriate FDC. Any message number not contained in the acode2fdc table must be manually added and mapped to an FDC.

- ASP Messages

  5ESS Advanced Services Platform (ASP) DSEs (direct signalling events) report Advanced Intelligent Network (AIN) call failures on 5ESS switches. In acode2fdc, map the ASP D field to the acode field and the ASP B field to the fname field. If there is no D field in a received ASP CIM, the converter performs a lookup on the B field.

- Any switch type using caus codes.

  For some switch types NTP does a secondary (fname) lookup on caus codes, to assign Fdc's matching cause codes. For these, use:

  – Acode of the caus code (this you must do)

  – Fname of ss7 (this you must do)

  – FDC of ccsx where x is caus code (these are suggested names—must be predefined in the Fdc table)

Example

```
#Acode; Fname; Fdc

1; SS7; ccs1

2; SS7; ccs2

3; SS7; ccs3

etc.
```

For a complete list of caus codes see "cause indicators" in the "ISUP Formats and Codes" chapter in Bellcore document GR-246-CORE.

adjarch Table

Purpose

The adjunct architecture (adjarch) table defines the network elements that are adjunct to switches.

Field dependencies

In table...	Before you put a value in field...	That value must be in field...	In table...
adjarch	swclli	clli	swarch
	stp	ne	stparch

Important! The adjclli field must contain a unique value which is not defined in a field in one of the following tables:

- swarch.clli
- stparch.ne
- lrarch.clli
- rtarch.rt
- ecosarch.area

adjroute Table

Purpose

This table identifies distant entities for each reporting adjunct entity. It contains digit based routing of the adjunct to switches.

Field dependencies

In table...	Before you put a value in field...	That value must be in field...	In table...
adjroute	adjclli	adjclli	adjarch
	signet	name	signet

alert_levels

Purpose

The alert_values table is used to define what quantity a given alert is measuring. Typically (and by default), this is simply a count of records. Other calculated values such as sums or averages of column values are possible. This table defines alert type, alert level, and minimum severity.

Notes

- By default, the AL field in each alert is assigned the AL value assigned to the alerted FDC in the FDC table. The AL field will receive the value in the AL column corresponding to the highest MIN_SEV value that the alert's severity value exceeds. This is a key field in the alert_levels table. Valid values for this field are: "cr" - critical, "ma" - major, "mi" - minor.
- If rows are added to the ALERT_LEVELS table for a given alert type, the severity of a new alert will be compared to the MIN_SEV values defined for that alert type in the ALERT_LEVELS table. The min_sev field can range from 0 to 9999. "-" is a valid value that indicates the field is not applicable or there is no data available.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
alert_levels	alert_type	type	alertdef

alert_notify Table

Purpose

The alert_notify table stores alert notification information.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
alert_notify	notify_id	notify_id	notify
	tablename	tablename	menutables

Table structure

The alert_notify table have the following structure:

Field name	Size	Field description
alertname	varchar2(20)	This field contains the name of the alert. This is the key field in the alert notify table.
searchexp	varchar2(4000)	This field contains a search expression used with a ‘sui find’ command.
notify_id	varchar2(20)	This field contains a unique notification id. This value must exist in the notify_id field of the notify table.
tablename	varchar2(30)	This field contains the tablename. This value must exist in the tablename field of the menutables table.
format	varchar2(200)	Optional. This field contains a format used with a ‘sui find’ command.
delimiter	varchar2(1)	Optional. This optional field holds the delimiter to be used in the sui command used to generate the alert.
runflag	varchar2(1)	This field indicates whether this search expression will be executed or not. The valid values are "y" (yes) or "n" (no).
repeattime	number(5)	This field determines how often (in minutes) this alert should be sent to the user. The default is 15 minutes. Values will effectively be rounded up to the next 5 minute interval.
subject	varchar2(30)	Optional. This optional field contains the subject for any email sent to a user for this alert notification.

Field name	Size	Field description
lastalert	date	Optional. This field contains the last date and time this alertnotification was sent to the user.
owner	varchar2(20)	Optional. This field contains the person who created this alert notification.

alertdef Table

Purpose

The alertdef table defines all the alert types in use.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
alertdef	srcmodel	model	chron_info

alertfq Table

Purpose

The alertfq table defines the FQ (fundamental quantity) for an alert type.

Important! Fieldname is a key field in this table. It can contain a string of 30 printable characters.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
alertfq	type	type	alertdef

alertperiods Table

Purpose

The alertperiods table defines all the periods for which an alert type is active.

Important! The closecai1, closecnt, and closecai2 fields are used for auto-close acases.

Notes

- Period is a key field in this table. This field defines the length of a period in minutes. The period field can range from 1 to 10080.
- For the min_thresh field, we suggest a value of 1. A higher value may improve capacity, but will cause lower volume FQs to be tracked less closely.
  FQs with thresholds below the min_thresh level are not tracked.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
alertperiods	type	type	alertdef

assert2fdc Table

Purpose

This table contains the assert code to fdc translations for 5ESS Assert messages. It is used to determine the fdc for the assert. The error codes for the asserts may change from release to release. Therefore, this table may need to be updated when the 5ESS switch is upgraded.

Important! ErrorCode and Release are key fields in this table.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
assert2fdc	fdc	fdc	fdc

atb_alerts Table

Purpose

The atb_alerts table is associated with the optional Trunk Busy Notification feature. It lists which alert types are tracked for atb notifications.

atb_digits Table

Purpose

The atb_digits table is associated with the optional Trunk Busy Notification feature. It contains digits of the REs to be tracked for allbsy failures notification.

atb_entities Table

Purpose

The atb_entities table is associated with the Trunk Busy Notification feature. It contains CLLIs of REs to be tracked for allbsy failures notification.

atb_log Table

Purpose

The atb_log table is associated with the optional Trunk Busy Notification feature. It logs all atb notifications and errors.

atb_troubles Table

Purpose

The atb_troubles table is associated with the optional Trunk Busy Notification feature. It contains a definition of trouble conditions to be monitored.

bdrhost Table

Purpose

The bdrhost table names hosts in the host pair for the RDS (reference data synchronization, refsynch). No entries are needed in this table unless you use RDS.

Important! Records for only two hosts (the RDS host pair) can be entered in this table.

Field dependency

None.

Reference

See Chapter 12, "Reference Database Synchronization (RDS)" for a full explanation of RDS.

See also the bdrhost field in the "source Table" (p. A-149).

bearch Table

Purpose

This table contains the billing entity pick lists for reporting.

Note

The key fields are **`bill_entity`** and **`description`**. The first defines the billing entity that can receive an output file from Billdats, and the latter provides a description of the billing entity.

Field dependency

None.

bgcf_reference Table

Purpose

This table is associated with the Border Gateway Control Function components (such as those in the Lucent Session Manager, which is an integral part of the Lucent IMS solution).

The BGCF Reference Data table includes reference data associated with BGCFs.

Field dependencies

In table...	Before you put a value in field...	That value must be in field...	In table...
bgcf_ reference	clli	re	rearch
		clli	swarch

bordelempair_reference Table

Purpose

This table is associated with Border Element Pairs. The members of these pairs could be Media Gateways (such as the Lucent Network Gateway) or Session Border Controllers (such as the Acme Packet Net-Net Session Director).

busy_hour Table

Purpose

The busy hour table contains a summary of all busy hour records (each RE type has a daily Busy Hour table).

The busy hour is the hour with the maximum value for some count, metric, measurement, raw data or KPI. For our purposes, an hour starts on an hour boundary (i.e. 12:00) and extends to the next hour boundary. Busy hour calculations are available on the following day. That is, there are no busy hour records for today.

carrier Table

Purpose

Maps a service carrier name (such as MCI), to a cic code. Cic codes are defined here, so they can be used in the ixcarrier table, which maps multiple cic codes to one customer (see “ixcarrier Table” (p. A-87)). Cic codes appear in several summary reports (if additional traffic analysis is implemented on your system).

Field dependency

None.

ccconfig Table

Purpose

Use if you have RE's from any of the following conversions:

- GeoProbe
- AXE 10
- AXE TRADO
- Lucent Softswitch
- IPDR
- Sonus
- CCF Charging Collection Function
- PCMD

The collectors table, along with the "fileconfig Table" (p. A-76), selects internal process to translate and CDR and IPDR CIMs to CFIMs.

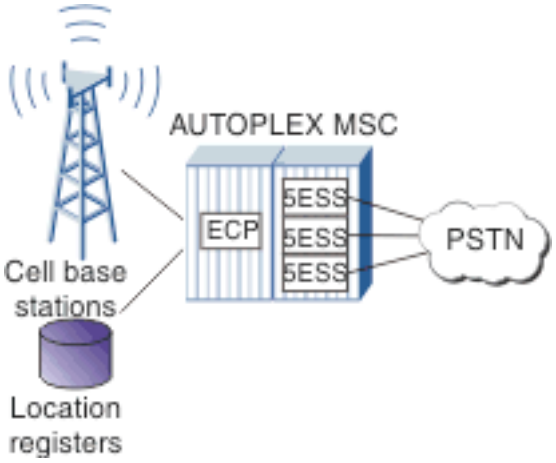
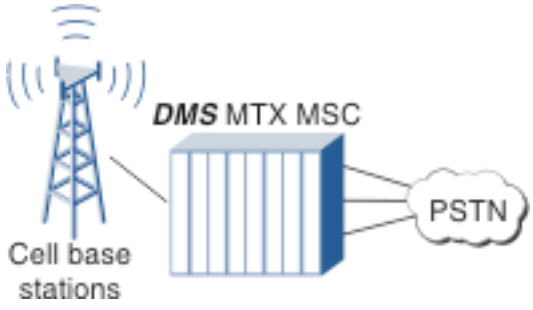
Field dependencies

In table...	Before you put a value in field...	That value must be in field...	In table...
ccconfig	source	name (must *match* value in source field in ccconfig table)	source
	conversion_name	conversion_name	bildtsrec (internal table)

cellroute Table

Purpose

Use if an RE is AUTOPLEX MSC or DMS MTX MSC. This table defines distant entities (DE's), when the RE is a mobile switching center (MSC). In detail:

If the RE is:	Cellroute table defines the DE's that are...	And OTHER DE's may be...
AUTOPLEX MSC	• Cell base stations Cell base stations are groupings of radios and other equipment, usually near an antennae. • 5ESS switch modules in the AUTOPLEX MSC (actually, these are internal to the MSC) *Illustration.* 	• Location registers, defined in the "num_std_rule Table" (p. A-116). (DE thresholding is turned on or off here, via the Ai field.) • PSTN switches, defined in the "route5e Table" (p. A-133). (DE thresholding is turned on or off here, via the Ai field.)
DMS MTX MSC	• Cell base stations *Illustration* 	• PSTN switches, defined in the "dmsroute Table" (p. A-58). (DE thresholding is turned on or off here, via the Ai field.)

Thresholding

Other route tables (dmsroute, etc.) have a corresponding "arch" table (with an Ai field where you turn thresholding on or off. There is NO cellarch table. Instead, use the Ai field in the swarch table. In the swarch table, see records that have, in the Eqtype field, either:

- base — For AUTOPLEX MSCs
- dms-mtx — For DMS-MTX MSCs

Field dependencies

In table...	Before you put a value in field...	That value must be in field...	In table...
cellroute	clli	re	rearch
	de	clli	swarch

celltype Table

Purpose

The celltype table contains a list of keywords found in CIMs and their corresponding cell types. This table is used with wireless features to identify the type of cell involved in a call failure message. (This table is populated during installation when the Autoplex HEH Support feature is enabled.)

Field dependency

None.

cell_ref_data Table

Purpose

The cell_ref_data table defines cell components in the UMTS network and their relationship to a NodeB.

Field dependencies

In table...	Before you put a value in field...	That value must be in field...	In table...
cell_ref_ data	cell	clli	swarch
		re	rearch
	utran_id	utran_id	nodeb_ref_ data
	rnc_id	rnc_id	nodeb_ref_ data
	nodeb	nodeb	nodeb_ref_ data

cgf_ref_data Table

Purpose

The cgf_ref_data table defines CGF components in the UMTS network.

Field dependencies

In table...	Before you put a value in field...	That value must be in field...	In table...
cgf_ref_ data	cgf	clli	swarch
		re	rearch

city Table

Purpose

The city table is used to identify valid city codes or NPAs for a particular country.

Recall that the CFIM's city_npa field shows a city code (international numbering plans) or NPA (North American Numbering Plan).

If city code or NPA is found in CDR field 46, NTP puts that value in the CFIM's city_npa field, and the city table is NOT used.

But if field 46 is blank, NTP uses the CDR's dsdigits (digits, if dsdigits is not available) and the city table to derive the CFIM's city_npa.

This derivation sometimes uses the following two swarch fields, which you need to populate:

- ccd
- hnpa

(All the above also applies to deriving the CFIM's cpcity_npa field, if not available in CDR field 45.)

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
city	ccd	ccd	country

cmdgroup Table

Purpose

The command group (cmdgroup) table lists command groups so that you can then use the "cmdgroupmap Table" (p. A-41) to define a set of commands in each command group. Then you can assign users to command groups to restrict user access to the NTP system.

Important! This table does NOT affect the BB-GUI. It affects only the SUI.

Reference: For procedures to define command groups, see "Create a command group" (p. 7-10).

Field dependency

None.

cmdgroupmap Table

Purpose

The command group map table defines the commands in command groups listed in the "cmdgroup Table" (p. A-40). You can then assign users to command groups to restrict user access to the NTP system.

Important!

- Command groups are NOT used in the BB-GUI.
- This table does NOT affect the BB-GUI. It affects only the SUI.

Reference: For procedures to define command groups, see "Create a command group" (p. 7-10).

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
cmdgroup-map	cmdgroup	name	cmdgroup
	command	name	command

code2text Table

Purpose

The code2text table is used to translate numeric and text codes in records into text strings for storage in the CFIM record.

Field dependency

None.

command Table

Purpose

The command table to contains a list of the commands in the system. It lists command names, descriptions, and whether or not the command can be listed on a command menu.

Field dependency

None.

cos Table

Purpose

Use the cos (class of service) table if you have 4ESS switches, and want to see their St fields populated more accurately. This table more accurately populates the St field on 4ESS CFIMs as follows:

- NTP takes the SII (service indicator index) from the 4ESS CIM and looks it up in this cos table, to find the matching St value.
- If the SII is not found in the cos table, use the old method to derive St.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
cos	st	type	st

country Table

Purpose

To populate the CFIM's ccd field, where the RE is:

- 4ESS (Improved ccd derivation)
- Any from GeoProbe
- Lucent Softswitch

NTP users can also use this table as a reference, to see which country codes represent which countries.

Field dependency.

In table...	Before you put a value in field...	That value must be in field...	In table...
country	npt	npt	npt

count_def Table

Purpose

The count_def table is associated with the optional Motorola iDEN Support feature. It contains all counts to be processed.

Reference: See "Add Motorola iDEN Count" (p. 4-98) for more information.

cs_admin Table

Purpose

The cs_admin table is used in the administration of Configurable Summarizers (optional feature). This table is populated via the **cs_create** and **cs_stat** commands. See Chapter 13, "Configurable Summarizers".

Field dependency

None.

cscf_reference Table

Purpose

This table is associated with the Call Session Control Function components (such as those in the Lucent Session Manager, which is an integral part of the Lucent IMS solution).

The CSCF Reference Data table includes reference data associated with P-CSCFs (Proxy Call Session Control Function), I-CSCFs (Interrogating Call Session Control Function), and S-CSCFs (Serving Call Session Control Function).

Field dependencies

In table...	Before you put a value in field...	That value must be in field...	In table...
cscf_ reference	clli	re	rearch
		clli	swarch

ctcode2ct Table

Purpose

Use this table if RE is from:

- IPDR
- Lucent Softswitch
- Custom added.

The ctcode2ct (call type code to call type) table identifies call types based on service or feature codes, or other unique identifiers. Specifically, NTP takes a code from a CDR or IPDR, looks it up the ctcode field of this table, and places the record's matching ct value in the CFIM's ct field.

Field dependency

None.

custcode Table

Purpose

It is nice to see the customer's name in the CFIM's Cust field, but the name is not on CIMs. But CIMs give other information, which you can map to a name, to populate the Cust field. Map in the following tables (different conversions use different sets of these tables):

- "custcode Table" (p. A-50) — Use this if you get RE's from IPDRs. Maps each customer's name to account codes, subscriber ids, or other unique identifiers. Populates both Cpcust and Cust fields on CFIM's.
- "custid Table" (p. A-51) — maps each IDB/DSD or other non-VPN customer's name to a phone number. If no match is found, the CFIM's Cpdigit's value is placed in Cust.
- "vpnid Table" (p. A-166) — maps each VPN customer's name to a VPN. If no match is found, the VPN is placed in Cust.
- "custip Table" (p. A-52) — maps each customer's name to an IP address.

Field dependency

None.

custid Table

Purpose

Not yet used for standard conversions, but available for CDR-type installations.

It is nice to see the customer's name in the CFIM's Cust field, but the name is not on CIMs. But CIMs give other information, which you can map to a name, to populate the Cust field. Map in the following tables (different conversions use different sets of these tables):

- "custcode Table" (p. A-50) — Use this if you get RE's from IPDRs. Maps each customer's name to account codes, subscriber ids, or other unique identifiers. Populates both Cpcust and Cust fields on CFIM's.
- "custid Table" (p. A-51) — maps each IDB/DSD or other non-VPN customer's name to a phone number. If no match is found, the CFIM's Cpdigit's value is placed in Cust.
- "vpnid Table" (p. A-166) — maps each VPN customer's name to a VPN. If no match is found, the VPN is placed in Cust.
- "custip Table" (p. A-52) — maps each customer's name to an IP address.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
custid	custname	cust	customer

custip Table

Purpose

Not yet used for standard conversions, but available for CDR-type installations.

It is nice to see the customer's name in the CFIM's Cust field, but the name is not on CIMs. But CIMs give other information, which you can map to a name, to populate the Cust field. Mapping uses the following tables (different conversions use different sets of these tables):

- "custcode Table" (p. A-50) — Use this if you get RE's from IPDRs. Maps each customer's name to account codes, subscriber ids, or other unique identifiers. Populates both Cpcust and Cust fields on CFIM's.
- "custid Table" (p. A-51) — maps each IDB/DSD or other non-VPN customer's name to a phone number. If no match is found, the CFIM's Cpdigit's value is placed in Cust.
- "vpnid Table" (p. A-166) — maps each VPN customer's name to a VPN. If no match is found, the VPN is placed in Cust.
- "custip Table" (p. A-52) — maps each customer's name to an IP address.

Field dependency

None.

customer Table

Purpose

Not used for standard conversions, but available for custom installations. Identifies customers.

Field dependency

None.

dcode2d Table

Purpose

Use if you get RE's from AXE 10. Derives CFIM's D (direction) field.

This is one of four tables (dcode2d, scode2sig, stcode2st, id2ne) used to translate Arbor BP CIMs to CFIMs. Tables fdc and acode2fdc are also used.

Reference: See "When to add or modify an FDC" (p. 4-76) for when this table is used.

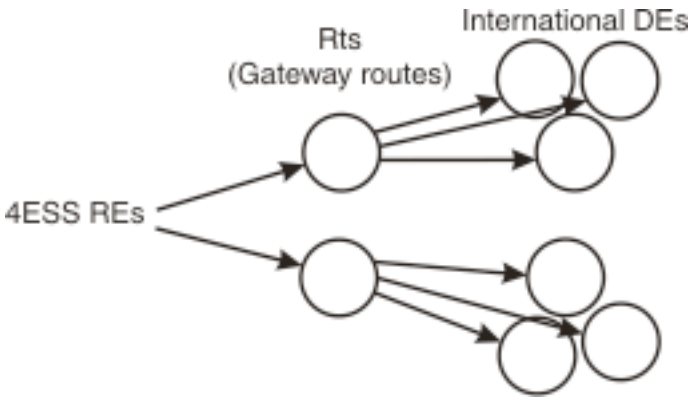
Field dependency

None.

de2route Table

Purpose

Use if you have 4ESS RE's, and you want to populate the Rt field (country gateway route) on 4ESS CFIMs. This table tells which Rt's go to which international DE's, as illustrated below.



Rtarch and De2route tables define the Rt field for 4ESS switches only. (Lucent Softswitch, also populates the CFIM Rt field, but does NOT use Rtarch and De2route tables.)

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
de2route	rt	rt	rtarch

Important! *NEMOS*. One customer only can update this table from a NEMOS database. See your NTP support organization for how.

Reference: Updating this table is explained at "Correct Wrong or Missing Rt Values" (p. 4-52).

dialingcode Table

Purpose

The dialingcode table contains a list of dialing codes.

Field dependency

None.

disabledig Table

Purpose

The disabled digit (disabledig) table tells the NTP system which FDC and digit patterns to ignore for alerting.

That is, if an FDC and digit pattern is listed in this table, then CFIMs with that FDC and called digit pattern are NOT tallied into CFIM counts (CFIM counts are compared to thresholds, and when thresholds are exceeded, an alert case is created.)

Network Entities represented in the CFIM (RO and DE) are not pegged if the corresponding FDC and digits if the CFIM matches the FDCs and digit patterns in this table.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
disabledig	fdc	fdc	fdc

dmsroute Table

Purpose

This table identifies distant entities for each reporting DMS entity. It matches DMS trunk groups with distant entities. Use this table if an RE is:

- DMS
- DMS MTX
- Succession SN05 and SN06
- Nortel GSM MSC

Important! Switching the Trunk Group Suffix feature on enables the user to identify trunk groups more easily, because of the suffix field (sfx) that is added to the cfim record. For more information on the Trunk Group Suffix feature, see Chapter 5 "Trunk Group Suffix (Sfx)" (p. 4-58).

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
dmsroute	clli	re	rearch
	de	clli	swarch
	sig	type	signaling

domain Table

Purpose

The table maps 4ESS domains to service types. Update only if 4ESS vendors change these. Use this table only if you have 4ESS RE's.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
domain	npt	npt	npt
	st	type	st

ecosarch Table

Purpose

Only one customer uses this table for ECOS. ECOS (end-to-end Class of Service) is a way to group calls by some criteria, so NTP can treat each grouping (called an "area") as if it were a DE. Each "area" can be domestic or international. The ecosarch table turns DE thresholding on or off for ECOS areas. (There is no RE thresholding for ECOS.)

Field dependency

Important! The area field must contain a unique value which is not defined in a field in one of the following tables:

- swarch.clli
- stparch.ne
- lrarch.clli
- rtarch.rt
- adjarch.adjclli

Reference: NEMOS. One customer only can see NEMOS documents for an explanation of ECOS. Update the Ecosarch table when the NEMOS ECOSREF table changes, as follows:

Get this value for the Ecosarch table...	From this column in the ECOSREF table in NEMOS...
area	tid

ecosroute Table

Purpose

Only one customer uses this table for ECOS. This table identifies distant entities for each RE. ECOS (end-to-end class of service) is a way to group calls so NTP can treat each grouping (called an "area") as if it were a DE. Each area can be domestic or international.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table
ecosroute	re	re	rearch
	area	area	ecosarch

Reference: See NEMOS documents for an explanation of ECOS. Update ecosroute when the NEMOS ECOSREF table changes, as follows:

Get this value for the ecosroute table...	From this column in the ECOSREF table in NEMOS...
re	fid
re	exid
area	tid

eqtype Table

Purpose

The equipment type table lists and describes equipment types. You must define an eqtype here before you can enter it in the eqtype field of the swarch table, so it can appear in the RE and DE fields of CFIMs. (You are NOT required to define an eqtype here before using it in the eqtype field of the Fdc table. But it is a good thing to do, to document each type's description.)

You can define any equipment type you need. NTP pre-populates this table at installation time with recommended values for common types. We recommend you use the appropriate pre-populated value, when available. (You may see a eqtype of univ. We suggest you do not use it. See “eqtype Table” (p. A-62).)

Field dependency

None.

ess1a2fdc Table

Purpose

The 1A ESS FDC (ess1a2fdc) table defines which FDCs appear on 1A *ESS* CFIMs.

Unlike CIMs from 4ESS, and 5ESS switches, the 1A *ESS* TN08 does not provide a single field describing the failure or event type. The TN08 is a cryptic message that requires an examination of several fields to determine the type of failure or event that occurred.

This table takes this combination of TN08 fields and converts them into an FDC to populate the CFIM and to use for thresholding. With this table, you can control how the FDCs are named and grouped for 1A *ESS* switches. This table is also used for translating CCS7 MESSAGE RTN, CCS7 UNKNOWN POINT CODE, and SCP ALERT messages from 1A ESS switches.

Reference: See "When to add or modify an FDC" (p. 4-76) for when this table is used.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
ess1a2fdc	fdc	fdc	fdc
	sig	type	signaling

Key fields

A tilde (~) used in any key field means:

- To fill in a field which doesn't apply to the message type in this record
- To act as a "wildcard" meaning match any value in this field, including a missing value. This makes it unnecessary to have a record exactly matching every possible message. The tilde will match a record where the field has no value. For example, the *q* , *r* , and *s* fields of TN08 messages do not exist in every TN08 message.

Use tildes in fields that you do not consider significant enough to translate uniquely. However, beware of introducing ambiguity into the ess1a2fdc database table by too generous use of wildcards. For example, certain TN08s could match either of the following records:

```
Type f q g e h r s d a FDC TC Dir Sig Failinfo
tn08 1 ~ 5 3 1 ~ ~ ~ ~ tgf oto o mf tgf,rvr,ddf,2st,eoh
tn08 1 2 5 3 1 ~ ~ ~ ~ xst oto o mf icto
```

A precedence rule in this situation selects the record with an exact match in the highest priority key fields to be the one used in a translation. Priority is determined by field order; the first field is highest priority. In the example, the second record would be used for a translation of a message with a value of 2 in the q field.

(A dash (-) in non-key fields means "no value" or "don't know".)

Important! The CCS7 UNKNOWN POINT CODE message is indicative of one specific failure or event type only; for this reason, it has only one record in this table.

Reference: For explanations of 1A ESS messages and fields, refer to the *1A ESS Output Manual,* (OM-6A001-01) , May 1993 or later.

event_status Table

Purpose

This table stores a status of test execution.

Field dependency

None.

ewsdroute Table

Purpose

This table identifies distant entities for each *EWSD* RE. The *EWSD* route table shows how other switches are connected to your *EWSD* switches. When NTP receives a CIM from an *EWSD* RE, NTP reads it to get the trunk group used, and then uses this table to determine the DE. NTP then puts that DE in the DE field of the CFIM it created from the CIM. (Otherwise, the DE field will say "?".)

Important! Switching the Trunk Group Suffix feature on enables the user to identify trunk groups more easily, because of the suffix field (sfx) that is added to the cfim record. For more information on the Trunk Group Suffix feature, see Chapter 5 "Trunk Group Suffix (Sfx)" (p. 4-58).

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
ewsdroute	clli	re	rearch
	de	clli	swarch

fcause Table

Purpose

The failure (event) cause (fcause) table defines reason codes so system users can enter those codes in the Fcause field of alert cases. They would enter these codes to classify Alert Cases, if desired.

Field dependency

None.

fdc Table

Purpose

The final disposition code (fdc) table defines FDCs.For some entities, this is a straight mapping. For 4ESS and 5ESS CIMs, this is a straight mapping of 4ESS FHCs and 5ESS MDIIs. For some types of switches, call failure or event information from switch messages must be put together and mapped to FDCs via intermediate database tables such as acode2fdc. The FDCs to which they are mapped must be defined in the fdc table before they can be used in the intermediate tables.

Reference: See “acode2fdc Table” (p. A-9) , for more about creating FDCs.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
fdc	sig	type	signaling
	st	type	st

Important! *CCS FDCs* . For conversions that map FDCs to caus codes, including GeoProbe, we pre-loaded records similar to these listed below. These FDCs are named "ccs..." with Sig of ccitt7, and with the same FDC in acode2fdc. Codes are defined for "cause indicators" in the "ISUP Formats and Codes" chapter in Bellcore document GR-246-CORE. Updates these if the reference changes.

```
#Fdc; Tc; Eqtype; Al; S; D; Sig; St; Tm; Ai; Mc;
ccs1; ccs; -; mi; f; o; ccitt7; -; p; on; n
ccs2; ccs; -; mi; f; o; ccitt7; -; p; on; n
ccs3; ccs; -; mi; f; o; ccitt7; -; p; on; n
etc.
```

fdc_eqtype Table

Purpose

The fdc_eqtype table is associated with the FDC Audit feature. It defines the FDC values to be audited.

Populating fdc_eqtype

The initial population of the **fdc_eqtype** table (when the table contains no rows) can be done:

- automatically by executing the **init_fdceqtype** script,
- manually through the **dbedit** command (it allows for modification, deletion, or insertion of any row in the table).

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
fdc_eqtype	fdc	fdc	fdc
	eqtype	type	eqtype

fdc_sev Table

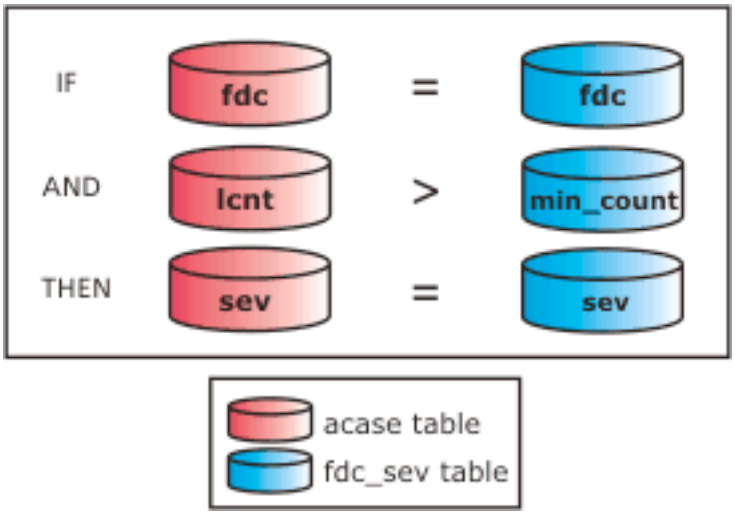
Purpose

This table is used with the optional Dynamic Alert Level based on FDC and Lcnt feature.

The fdc_sev table is used by the alerting process to dynamically update the severity of an alert case every 5 minutes. This allows certain failures to be designated as more or less serious than others.

Example: You might lower the severity of a certain alert case that normally would be considered a failure, but under certain circumstances is considered normal.

This illustration shows how the severity of acase is updated.



1. Use the fdc_sev table to specify a min_count and severity for a particular FDC.
2. The alerting process changes the sev field in an alert case to the severity value in the fdc_sev table if:
   - the FDC in the alert case matches an FDC in the fdc_sev table, and
   - the lcnt value in the alert case exceeds the min_count value specified in the fdc_sev table.

   Important! If there are multiple records in fdc_sev for a particular FDC, the one with the highest severity is used.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
fdc_sev	fdc	fdc	fdc

fdc2tn Table

Purpose

This table contains FDC mappings for TN grouping to be done automatically by the system. It maps an FDC defined in the FDC table with a type of network entity.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
fdc2tn	fdc<*number*>	fdc	fdc

fdcgroup Table

Purpose

The FDC group (fdcgroup) table lists FDC groups so that you can then use the "fdcgroupmap Table" (p. A-73) to define the set of FDCs in each FDC group. Then you can assign users to FDC groups to help limit the output users see.

Reference: For procedures to define FDC groups, see "Create an FDC group" (p. 7-19).

Field dependency

None.

fdcgroupmap Table

Purpose

The FDC group map (fdcgroupmap) table defines the FDCs in each FDC group listed in the "fdcgroup Table" (p. A-72). You can then assign users to FDC groups to help limit the output users see.

Reference: For procedures to define FDC groups, see "Create an FDC group" (p. 7-19).

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
fdcgroup-map	fdcgroup	name	fdcgroup
	fdc	fdc	fdc

helptext Table

Purpose

The helptext table provides descriptions of fdc (final disposition codes), column and tooltips. .

Reference

- For the procedure to of managing the helptext table, see "Manage Help Texts" (p. 9-18).

Field dependency

None.

fdcpermit Table

Purpose

The FDC permit (fdcpermit) table defines which FDC groups users can see. This table is modified when a new user is added and assigned to an FDC group other than "all". It is also modified when a user who has been assigned to all FDC groups is given a particular FDC group assignment.

Important!

- This table does NOT affect the BB-GUI. It affects only the SUI.
- FDC assignments for the BB-GUI are handled separately through the Web User Information page.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
fdcpermit	fdcgroup	name	fdcgroup

fileconfig Table

Purpose

The fileconfig table, along with the "ewsdroute Table" (p. A-66), selects internal processes to translate CDR and IPDR CIMs to CFIMs for the NTP configurable converter interface. (It is also used for some universal conversions). Use this table for:

- GeoProbe
- AXE 10
- AXE 10 TRADO
- Lucent Softswitch
- IPDR
- Sonus
- CCF Charging Collection Function
- PCMD

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
fileconfig	source	source (must match value in source field in fileconfig table)	ccconfig

gtspec Table

Purpose

The global title specification (gtspec) table attempts to determine a CFIM's DE (and sometimes Related) value if all else fails (such as when the DE is not found in a routing table). It applies to all Retypes.

Important! If you modify this table, do so ONLY with assistance from your NTP support organization. Also, Review Chapter 11, "Update the gtspec Table", before attempting to make changes to this database table.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
gtspec	st	type	st

hoas_reference Table

Purpose

The hoas_reference table contains data associated with the HandOff Application Server feature.

Field dependencies

In table...	Before you put a value in field...	That value must be in field...	In table...
hoas_ reference	clli	re	rearch
		clli	swarch

hierarchy_def Table

Purpose

The hierarcy_def table defines relationships between components within a service providers network. The information is used to render a hierarchical view of network components in the BB-GUI.

homedigits Table

Purpose

Not used for standard conversions, but available for CDR-type installations.

The homedigits table is used to identify the local or wireless service provider using the called or calling party digits.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
homedigits	ccd	ccd	country
	cic	cic	carrier

id2ne Table

Purpose

Use if an RE is an AXE 10.

Derives each CFIM's RE (reporting entity) field or DE (distant entity) field from Arbor BP call detail records (CDRs).

That is, if the CDR identifies an RE or DE with a code other than a traditional 11-character CLLI, this table converts that code to a CLLI. Specifically, if the code on the CDR is not found in swarch (RE field), then NTP brings the code to the id2ne table to maps the code to a CLLI.

This is one of four tables (dcode2d, scode2sig, stcode2st, id2ne) dedicated to telling how to translate Arbor BP CIMs to CFIMs. Existing tables fdc and acode2fdc are also used.

Reference: See Step 13 in "Add or modify an FDC" (p. 4-78) for when this table is used.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
id2ne	ne	clli	swarch

intcpdial Table

Purpose

The incoming TCP dial (intcpdial) table defines all incoming TCP/IP interfaces to CIM sources. These interfaces can be defined by IP address, host name, or fully qualified domain name.

Sources in this table cannot appear in the outtcpdial table. This table is used to tell NTP to LISTEN for the source to send data over TCP/IP.

Reference: To tell NTP to REQUEST the source to send data over TCP/IP, see "outtcpdial Table" (p. A-119) .

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
intcpdial	source	name	source

Important!

- *Refsynch* . This table is not synchronized by refsynch (see Chapter 12, "Reference Database Synchronization (RDS)").
- *Sources* . Consult with your NTP support organization to determine which table to use for a given CIM source. See Chapter 5, "CIM Source Administration" for guidelines.

Examples

In this example, the NTP host listens over its TCP port 3011 for data from a source with host name source sim0, which is known to NTP by the source name source02. (You must get the source host name and port number from the source administrator.)

```
Source Active Origin1 Origin2
source02 y sourcesim0:3011 -
```

In this example, the same source is identified by IP address instead of host name.

```
Source Active Origin1 Origin2
source02 y 10.2.1.203:3011 -
```

internat_list Table

Purpose

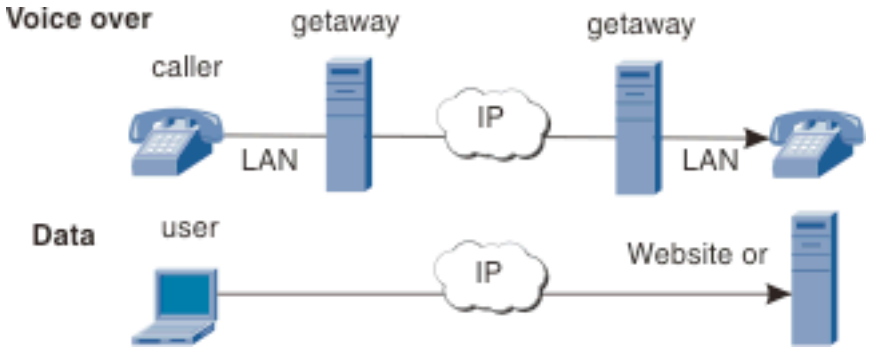
This table is used with the optional Digit Standardization feature.

The internat_list table contains a mapping of country codes and carrier assigned digit blocks to a country and the and the carrier that owns the digit block.

iparch Table

Purpose

Use if you have IPDR (internet protocol detail record) RE's. IPDRs report on data networks. NTP can process IPDR's as CIMs. This illustration shows typical networks monitored by a mediation system that creates IPDRs.



Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
iparch	owner	id	owner

ipservice Table

Purpose

The ipservice table enables identification of a specific service given an IP address. It defines such things as IP address, port, URL, and a description of service.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
ipservice	ipadress	ipadress	iparch
	st	type	st

isa_host Table

Purpose

This table is created to maintain a list of all trusted 8925 Integrated Service Assurance and Network Fault Management software hosts. The trusted hosts can request a connection with the NTP_ISA server to receive alertcase information. The table contains a single column (ISA_HostID) which can be up to 30 characters in length.

ixcarrier Table

Purpose

Use if you have RE's from Lucent Softswitch. Lucent Softswitch CIMs normally provide a CIC only if the call is routed through a transit (inter-exchange) carrier, such as MCI.

Use this to map multiple cic's to one carrier. For example, if carrier MCI (cic of 111111) has three IDs (aaaaaa, bbbbbb, and cccccc), enter the following in this table:

```
Ixcic      Cic
aaaaaa     111111
bbbbbb     111111
cccccc     111111
```

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
ixcarrier	cic	cic	carrier

journal Table

Purpose

The journal table is populated directly from journal records transferred from Arbor BP to NTP.

journalhour Table

Purpose

The journahour table is an hourly summarized version of the journal table.

Field dependency

None.

latacode Table

Purpose

The lata (local access and transport area) table identifies calling and called party LATAs. This table can be used in CDR-type installations to derive LATAs and areas.

Field dependency

None.

lrarch Table

Purpose

Use to define location registers, so they can be DE's, for RE's that are either:

- An OSPS module on a 5ESS AUTOPLEX.
- An OTR module on a DMS MTX MSC (and LNP)

This table is also used for Lucent Softswitch.

This table defines location register DE's. Location registers are not switches, but are databases used to authenticate wireless calls. They can not be RE's.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
lrarch	clli	clli	swarch

Important! The clli field must contain a unique value which is not defined in a field in one of the following tables:

- swarch.clli
- stparch.ne
- adjarch.adjclli
- rtarch.rt
- ecosarch.area

lrn2ne Table

Purpose

Used to derive the CFIM's Lrne field value, if an RE is:

- An OTR module on a DMS MTX MSC (and LNP)
- From Lucent Softswitch

The location routing number to network element (lrn2ne) table maps a location routing number to a network entity. If you see a "?" or an incorrect switch in a CFIM's Lrne field you may need to update this table.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
lrn2ne	ne	clli	swarch
		scpclli	scparch
		ne	stparch
		adjclli	adjarch
		area	ecosarch

Important! *Field dependency NOT enforced*. That is, even if you violate the rules in the table above, a dbedit update to the lrn2ne table's ne field WILL succeed. NTP leaves field dependency unenforced because you could also use a remote entity CLLI (in the lr2ne table's ne field), and there is no way to validate remote entity CLLIs. Even though field dependency is not enforced, you SHOULD ensure any CLLI used in the lrn2ne table's ne field is a valid CLLI--either according to the table above, or as a valid remote entity CLLI.

lspcalendar Table

Purpose

This table is used for alerting. The lsphours table assigns LSPs to each hour of each weekday, and each hour of Saturday and Sunday. But what if, for example, you want to threshold Labor Day (a Monday) as if it were a weekend? Use this table to override. You could also create a special day type (such as h for holiday) in the lspdays table, and assign it here.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
lspcalendar	datype	datype	lspdays

Reference: See Chapter 8, “Threshold Administration”.

Example

Here is a record saying to use weekend LSPs on Labor Day:

```
20000904 W Use weekend LSPs
```

lspdays Table

Purpose

This table is used for alerting to decide which days of the week are b (business), w (weekend), or other types you may create here. b and w are initial default types. You can have up to seven types.

Field dependency

None.

Reference: See Chapter 8, “Threshold Administration”.

lspdaytypes Table

Purpose

This table specifies the complete set of daytypes that can be assigned to a day of the week in lspdays, a date in lspcalendar, or an hour in lsphours.

- The daytype field defines a type of day used to set up load set periods.
- The soak field indicates the soak period for each daytype.
  The number in the soak field is interpreted as number of 5-minute periods. For example, 120, which is the default soak for b (business, see "lspdays Table" (p. A-94)), is interpreted as 120 5-minute periods. 48, which is the default soak for w (weekend, again see "lspdays Table" (p. A-94)) is interpreted as 48 5-minute periods.

  Important! Anytime the soak field value is decreased, thresholds for FQs that have a soak in progress may become erroneous. Use the **`set_resoak`** command to resoak any entities that have a soak in progress (see "Re-soak" (p. 8-27)).

Field dependency

None.

Reference: See Chapter 8, "Threshold Administration".

lsphours Table

Purpose

This table is used for alerting. It pairs each daytype with each hour, and assigns an ID to each pair. IDs are then used to create automatic thresholds for each period (in the mean_xx tables), or to assign a manual threshold (in the man_thresh_xx tables). In those tables, each Lspid actually consists of the pair of values in the first and last fields of this table.

Example

Since you have two initial default daytypes (b and w), and there are always 24 hours in a day (0 to 23), you must have 48 records, with the first two fields filled in as shown below. The third field you can fill in as shown, with a different Lspid for each "b" hour and for each "w" hour. This generates a different set of thresholds for each hour of "b" days, and each hour or "w" days.

```
Day Ho Lspid
b    0 0
b    1 1
b    2 2
b    3 3
```

(and so on, up to "b 23 23")

```
w    0 0
w    1 1
w    2 2
w    3 3
```

(and so on, up to "w 23 23")

In the Lspid field, you can reuse a number within the "b" hours, or separately within the "w" hours. For example, if you do this:

```
b    0 1
b    1 1
b    2 1
b    3 1
```

(and so on, up to "b 23 1")

```
w     0 1
w     1 1
w     2 1
w     3 1
```

(and so on, up to "w 23 1")

This generates just two sets of thresholds: A b1 set for all b hours, and a w1 set for all w hours.

In addition to all the bnumber and wnumber records, there will be one plain b record for the weekday daily mean, and one plain w record for the weekend daily mean.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
lsphours	datype	datype	lspdays

Reference: See Chapter 8, “Threshold Administration” .

man_thresh_xx Tables

Purpose

"Man_thresh_xx" refers to multiple tables, where xx is a alerting FQ. For example, for alerting on the cc FQ, there is a man_thresh_cc table.

Use this table to override NTP's automatically created thresholds, if desired. Initially, this table holds no records. You add or change records as follows:

To do this	Use this procedure	To put these values in thr, max and min
Set manual threshold to replace automatically created thresholds	"Manual thresholds" (p. 8-3)	A threshold value in thr. Max and min are ignored (so use "-" to remind you).
Limit how far a threshold can automatically adjust	"Limit LSP threshold adjustment" (p. 8-25)	A value in max, min, or both, in the same, or two records. You MUST put "-" in thr.
Turn off thresholds	"Turn off thresholds" (p. 8-34)	A "-" in thr, max and min.

Wildcards

In key fields, you can use "~" as a wildcard. A wildcard means "match all values".

Wildcards in key fields in different records may overlap. For example, in man_thresh_cc you could see two records with the following values:

- at=5m, lspid=~, fdc=abc, ccd=~, thr=99, min=~, max=~ This means, for 5 minute intervals, for ALL LSPs, for FDC of abc, for all ccds, use a threshold of 99
- at=5m, lspid=b1, fdc=abc, ccd=~, thr=11, min=~, max=~ Similar to above, but use threshold of 11 for LSP 1 ONLY.

So, the first record assigns threshold 99 to ALL LSPs, while the second assigns threshold 11 to LSP 1. And this is an overlap, assigning both 11 and 99 to LSP 1.

In this case, it is likely you really want to assign threshold of 99 to all BUT LSP 1, and threshold 11 to ONLY LSP 1—and that is how NTP interprets this overlap—as explained in the next table.

Precedence

For how NTP interprets overlaps, see the rules of precedence in the following table. Our example is for the cc FQ.

Key Fields ("~" is wildcard) at lspid fdc ccd	Non-key fields ("-" is a null) thr min max	Precedence
5m 10 abc 99	Anything	First, since there is no wildcard in a key field.
A wildcard ("~") in one or more fields.	- - -	Second, since "-" in all three is special, meaning no threshold.
	10 - -	Third, since a value in thr means any value in max or min is ignored. If more than one record is like this, use the smallest thr.
	- 5 10	Fourth. If more than one record is like this, use the smallest max and smallest min.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
man_thresh_xx	lspid	each unique pairing of values in the daytype and lspid fields, such as b0, b1, b2...w0, w1, w2...	lsphours
	FQ fields		

Note

- If you dbedit this table, for each lspid in records you edit, enter: buildthresh lspid If you fail to do this, manual thresholds you added will eventually take affect, but only AFTER the end of each affected LSP. Typically, this means waiting a week for a manual threshold to take affect.
- Key fields are: at, lspid, and all FQ fields. You can assign a different manual threshold for each unique combination of values in these fields.
- Changes to this table take affect on LSP boundaries. See “LSPs” (p. 8-18)
- Different man_thresh_xx tables are from different features.

Reference

- mean_xx. For each FQ there is a man_thresh_xx table and a mean_xx table (such as man_thresh_cc and mean_cc). See "mean_xx Tables" (p. A-102).
- See Chapter 8, "Threshold Administration".

manufacturer Table

Purpose

This table contains a list of mobile equipment manufacturer codes and names, along with a detailed description of the mobile equipment.

Important! This table is kept updated with each release. To update it more frequently, use dbedit (see "Dbedit" (p. 3-17)) to insert the ASCII file's records into the database.

Field dependency

None.

Reference

Access *http://www.tiaonline.org/standards/esn/codes.cfm* for information about the source of manufacturer codes for North America.

Access *http://www.tiaonline.org/standards/resources/meid/* for information about MEID reports from Telecommunications Industry Association.

mean_xx Tables

Purpose

"Mean_xx" refers to multiple tables, where xx is a alerting FQ. For example, for alerting on the cc FQ, there is a mean_cc table.

NTP uses this table to automatically create thresholds for alerting. That is, it accumulates a CFIM count in the count field, which NTP uses to create thresholds. (Thresholds are NOT shown here, but are in tables not visible to you.) For more details, see "Soaks" (p. 8-26).

Records in this table are automatically created, but you might dbedit the following fields in this table:

- accum — Enter a bigger value (up to maximum) to shorten a soak in progress. See "Shorten a soak in progress" (p. 8-29).
- accum and count — Enter 0 in both fields, to re-soak a threshold. See "Re-soak" (p. 8-27).
- frozen — After a soak is complete, thresholds are still adjusted at the end of each LSP. Edit the frozen field, to freeze or unfreeze adjustment. See "Freeze LSP threshold adjustment" (p. 8-24).

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
mean_xx	lspid	each unique pairing of values in the daytype and lspid fields, such as b0, b1, b2...w0, w1, w2...	lsphours
	FQ fields		

Note

- No wildcards. Wildcards are not used in this table. For what we mean by wildcards, see "Wildcards" (p. A-98).
- No "at" field? Each corresponding man_thresh_xx table has the same key fields, plus the "at" (alert interval type) key field. Why is "at" missing from mean_xx? Because, mean_xx does NOT show thresholds for each "at". Instead, mean_xx shows only the count, from which the thresholds are automatically created. Those thresholds (for each "at") are in tables not visible to you.
- Where are automatic thresholds? Not here. See previous item.
- Features. different mean_xx tables are from different features.

Reference

- man_thresh_xx. For each FQ there is a man_thresh_xx table and a mean_xx table (such as man_thresh_cc and mean_cc). See "man_thresh_xx Tables" (p. A-98).
- See Chapter 8, "Threshold Administration".

menutables Table

Purpose

The menu tables (menutables) table causes menu tables to appear in user interface menus.

The menutables table lists:

- Surveillance (output) tables, described in the *BB-GUI User's Guide*.
- User-modifiable reference tables, described in this appendix

  Important! Internal ("hidden") tables. If a table is NOT listed in menutables, you can assume it is modified by internal processes and is not meant to be user-modifiable. See “Internal ("hidden") tables” (p. A-6) for more information on these tables.

Field dependency

None.

mt20route Table

Purpose

The mt20route table contains a mapping of re trunk groups to a corresponding de.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
mt20route	clli	re	rearch
	de	clli	swarch

mgcf_reference Table

Purpose

This table is associated with the Media Gateway Controllers (such as the Lucent Network Controller-P/MGCF-P or the Lucent Network Controller-LCP/MGCF-LCP).

mg_reference Table

Purpose

The MG Reference Data table includes reference data associated with Media Gateways (MGs).

netgroup Table

Purpose

The network group (netgroup) table lists network groups so that you can then use the "netgroupmap Table" (p. A-109) to define the network segments in the groups. You can then assign users to network groups to help limit the output they see.

Field dependency

None.

Reference: For procedures to define network groups (and segments), see "Define Network Groups and Segments" (p. 7-34).

netgroupmap Table

Purpose

The network group map (netgroupmap) table lists the network segments in the network groups listed in the "netgroup Table" (p. A-108). You can then assign users to network groups to help limit the output they see.

Reference

For procedures to define network groups (and segments), see "Define Network Groups and Segments" (p. 7-34).

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
netgroupmap	netseg	name	netseg

netpermit Table

Purpose

The network permit (netpermit) table defines which network groups and segments users can see. This table is modified when a new user is added and assigned to a group or segment other than "all". It is also modified when a user who has been assigned to all groups is given a particular segment or group assignment.

Important! This table does NOT affect the BB-GUI. It affects only the SUI.

Network group and segment assignments for the BB-GUI are handled separately through the Web User Information page.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
netpermit	sysuser	login	sysuser
	netseg	name	netseg or netgroup

nodeb_ref_data Table

Purpose

The nodeb_ref_data table defines NodeB components in the UMTS network and their relationship to an RNC.

Field dependencies

In table...	Before you put a value in field...	That value must be in field...	In table...
nodeb_ref_data	nodeb	clli	swarch
		re	rearch
	utran_id	utran_id	rnc_ref_data
	rnc_id	rnc_id	rnc_ref_data

netseg Table

Purpose

The network segment (neseg) table lists network segments so that you can then use the "netpermit Table" (p. A-110) to define the Ne's in each segment. You can combine network segments into network groups and assign users to groups to help limit the output they see.

Reference: For procedures to define network segments (and groups), see "Define Network Groups and Segments" (p. 7-34).

Field dependency

None.

netsegmap Table

Purpose

The network segment map (netsegmap) table defines which network elements (Ne's) are in the network segments listed in the "netseg Table" (p. A-112). You can then group network segments into network groups and assign users to groups to help limit the output they see.

Reference: For procedures to define network segments (and groups), see "Define Network Groups and Segments" (p. 7-34).

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
netsegmap	netseg	name	netseg
	ne	clli	swarch
		scpclli	scparch
		ne	stparch
		adjclli	adjarch
		clli	lrarch (AUTOPLEX)
		area	ecosarch

notify Table

Purpose

The notify table contains the list of responsible parties who are notified in the event of certain system failures and events. See “Alert notification” (p. 10-7) for information on the types of system events for which these parties will receive notification.

Table structure

The notify table have the following structure:

Field name	Size	Field description
notify_id	varchar2(20)	This field contains a unique notification id. This is a key field in the notify table.
notify_type	varchar2(4)	This field indicates the type of notification. Valid values for this field are: "mail" - notify with a mail message, "wall" - notify with a wall message, "log" - write to a log file, "prog" - send message to a program, "none" - no notification.
severity	varchar2(8)	This field indicates the severity of the message. Valid values for this field are: "critical" - critical error, "major" - major error, "minor" - minor error, "info" - informational message.
addressee	varchar2(200)	This field includes a comma separated list of email addressees or program location.

npt Table

Purpose

Use if you have 4ESS RE's. This table defines npt's (numbering plan types), so that:

- They can appear in the Npt field of 4ESS CFIMs.
- You can use them in the Npt field of the country table, which NTP uses to derive the Ccd (country code) field of 4ESS CFIMs.

Initially the npt table holds these records.

```
NPT;CIM_NPT;DESCRIPTION
nan;0;North American Numbering Plan
apn;1;Action Point Numbering Plan
int;-;International Numbering Plan
```

Field dependency

None.

num_std_rule Table

Purpose

This table is used with the optional Digit Standardization feature.

The num_std_rule table contains rules that are used by the production digits standardization engine. The rules indicate how to standardize a digit string and how to determine customer type.

oline2st Table

Purpose

This table maps ISUP originating line codes to service type, to populate the CFIM's St (service type) field and is used if you have the RE's from the following conversions:

- EWSD switches
- GeoProbe
- IPDR

GeoProbe. For GeoProbe, the following records must be in the oline2st table:

```
#Oline; St
1; oper
2; oper
3; oper
4; oper
5; oper
10; pots
12; data
15; coin
224; emerg
225; emerg
```

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
oline2st	st	type	st

otr2fdc Table

Purpose

This is an optional table. OTRs (operator trouble reports) can be mapped to FDCs and used in thresholding and alerting just as are any call failure or event messages. You can control how FDCs for OTRs are named and grouped. The otr2fdc table is installed with trouble codes 00-99 pre-installed.

Some OTR FDCs provided by TOPS LNP do not have to be defined in this table, but put them here anyway, if you want them to appear in the optional OTR table. You can recognize which TOPS FDCs to put here—they are the ones that use the CFIM's Opn and Opid fields.

Reference: See *Step 13* in "Add or modify an FDC" (p. 4-78) for when this table is used.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
otr2fdc	fdc	fdc	fdc

outtcpdial Table

Purpose

The outgoing TCP dial (outtcpdial) table defines all outgoing TCP/IP connections to CIM sources. Sources in this table cannot appear in the intcpdial table. This table is used to tell NTP to REQUEST the source to send data over TCP/IP.

Reference: To tell NTP to LISTEN for the source to send data over TCP/IP, see "intcpdial Table" (p. A-82) .

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
outtcpdial	source	name	source

Important!

- Refsynch. This table is not synchronized by refsynch (see Chapter 12, "Reference Database Synchronization (RDS)").
- Sources. Consult with your NTP support organization to determine which table to use for a given CIM source. See Chapter 5, "CIM Source Administration" for guidelines.

Example

In this example, the NTP host requests data from a source with host name source02 over that machine's port 18762. This source is known to NTP by the source name nts02. (You must get the source host name and port number from the source administrator.)

```
Source Active Dest1          Dest2  Redialmin Timeoutmin
nts02  y      source02:18762 -     3         15
```

pkt_core_ref_data Table

Purpose

The pkt_core_ref_data table is used to define a unique Packet Core identifier. It can be used to create a set of logical Packet Core networks based on regions and associate components that are within that region with the logical group.

owner Table

Purpose

This table identifies the owner of a network element, whether RE or DE. In other tables, such as swarch and iparch, you put owners in the owner field (to tell who owns what). Here the "id" field names each owner and the other fields define who each owner is.

Example

There should be a record in this table for your company. If your company is North East Telephone, the record would look like this:

```
id  name   type cic
NETNorth  East Telephone owner 123
```

There would also have to be a record for each interexchange carrier that your network interfaces to. A record for one customer would look like this:

```
id  name     type cic
XYZXY&Z  ic   288
```

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
ixcarrier	cic	cic	carrier

patrn2rule

Purpose

This table is used with the optional Digit Standardization feature.

The patrn2rule table contains "patterns" that are used by the production digits standardization engine to check incoming cim data and determine which entry in num_std_rule to execute. Checks may be performed on called and calling party digit lengths, called and calling party contents, and trunk group information. All defined checks executed and if they are all successful the appropriate rule in num_std_rule is executed and the resulting values are stored in the CFIM.

pc2clli Table

Purpose

Some CIMs identify network elements by point codes (PCs), so NTP needs to know how to translate PCs to CLLIs. If there is just one PC per CLLI, you can add the CLLI to swarch, with the PC in swarch's Dpc field. But it there are multiple PC's per CLLI, you would need to use this table.Currently this table is required for:

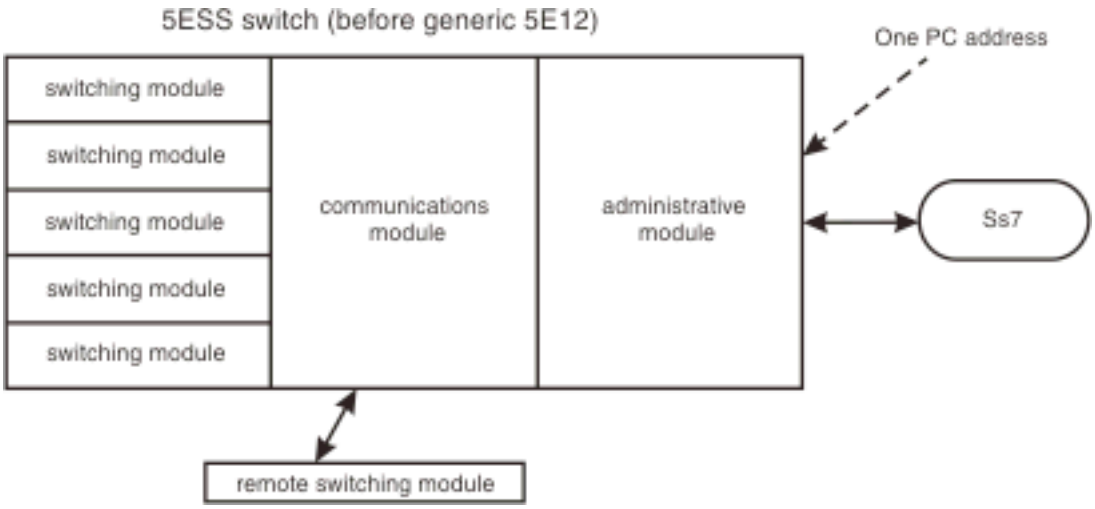
- GeoProbe
- 5ESS. Only 5ESS switches in generic 5E12 or later can have multiple PCs. The 5E12 multiple PC feature is called "SS7 PSU on SM/EXM2000"

If a switch has just ONE PC, we recommend you do NOT put the switch and its PC in this table. Instead, use the Dpc field of the swarch table.

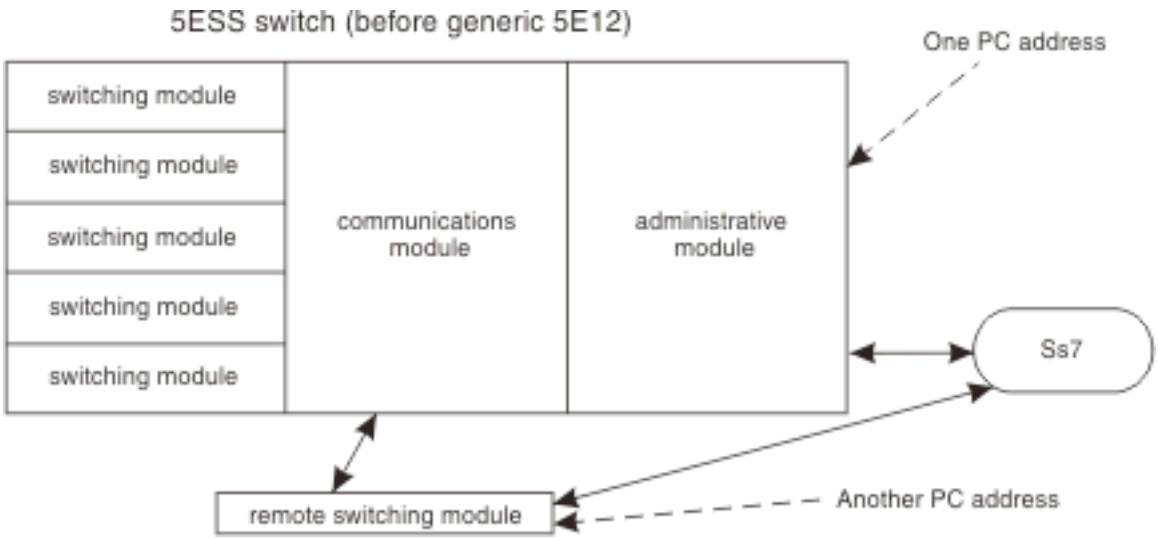
But, if a switch has multiple PCs, put all of the switch's PCs in this table. (If you do this, what do you use in the Dpc field of the swarch table? Use a dash, or repeat a PC. You could even put one PC in Dpc of the swarch table, and remaining PCs in the pc2clli table, but that would be cumbersome.)

5ESS Illustration

This illustration shows a 5ESS RE with one PC address.



This illustrates a 5ESS RE with multiple PC address. The switch can have a PC address for each remote switching module.



Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
pc2clli	clli	clli	swarch

potsroute Table

Purpose

Use if an RE is an:

- OSPS module on a 5ESS AUTOPLEX.
- OTR module on a DMS MTX MSC (and LNP)

The POTS route (potsroute) table contains the association of a 10-digits plain old telephone service (POTS) to a network entity (NE). The first six digits (NPA_NXX) are used to uniquely identify an end office. In some cases, the seventh digit is used to identify an end office.

This works on a best-match algorithm. For example: A potsroute record with the six digits 614860 specifies an area code and exchange; another record with the digits 6148607 might specify a specific PBX within that exchange. Use two or more records to specify such distinctions. A CIM with the digit string 6148607465 would point to the record with the PBX as the network entity. A CIM with the digit string 6148604487 would match a record for the exchange network entity but not the PBX.

Reference

See Step 13 in "Add or modify an FDC" (p. 4-78) for when this table is used.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
potsroute	ne	clli	swarch

pptemp_columns Table

Purpose

The pptemp_columns table is one of two tables that define templates that determine the graphical information displayed on Pattern Painter pages. (See also "pptemplate Table" (p. A-127).) Pattern Painter runs in association with the BB-GUI.

This table lists template name and table name, as well as all the fields Pattern Painter displays in the parabox for a particular template. This table also allows you to specify an order for the parabox columns. The pattern painter parabox display will present the data ordered by the values in the column_order column.

Important!

- This table affects Pattern Painter only.
- If you delete a template from the pptemplate table, the system automatically deletes that template from the pptemp_columns tables.

Background

The default template (see "pptemplate Table" (p. A-127) for the pptemplate table) includes the following cfim fields: cpdigits, re, de, tgn, digits, etime.

Reference:

- See "Customize Pattern Painter Displays" (p. 9-11) for when this table is used.
- See Appendix A in the *BB-GUI User's Guide* for information on the cfim table.
- See Chapter 7 of the *BB-GUI User's Guide*. for information on Pattern Painter pages.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
pptemp_ columns	template_name	template_name	pptemplate
	tablename	tablename	menutables

pptemplate Table

Purpose

The pptemplate table is one of two tables that define templates that determine the graphical information displayed on Pattern Painter pages. (See also "pptemp_columns Table" (p. A-126).) Pattern Painter runs in association with the BB-GUI. The graphics include two pie charts and a parabox.

Each entry in this table defines a template name and table name. The entry also specifies the fields that Pattern Painter displays in each of the two pie charts, as well as the fields that Pattern Painter uses to select colors in the display.

Important!

- This table affects Pattern Painter only.
- If you delete a template from the pptemplate table, the system automatically deletes that template from the pptemp_columns tables.

Default Template

The system provides a default template that Pattern Painter uses if no other templates are defined. (You cannot modify the default template.) Pattern Painter also uses the default template to display Finds involving multiple FDCs. But for Finds involving one FDC only, Pattern Painter uses whatever template you define for that FDC.

Reference:

- See "Customize Pattern Painter Displays" (p. 9-11) for when this table is used.
- For information on the cfim table, see Appendix A in the *BB-GUI User's Guide*.
- See Chapter 7 of the *BB-GUI User's Guide*. for information on Pattern Painter pages.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
pptemplate	tablename	tablename	menutables

rnc_ref_data Table

Purpose

The rnc_ref_data table defines RNC components in the UMTS network and their relationship to the UTRAN network.

Field dependencies

In table...	Before you put a value in field...	That value must be in field...	In table...
rnc_ref_ data	rnc	clli	swarch
		re	rearch
	utran_id	utran_id	utran_ref_ data

rearch Table

Purpose

The reporting entity architecture (rearch) table defines network entities that send CIMs to NTP. These must also be in the swarch table.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
rearch	re	clli	swarch
	source	name	source

Key fields

The re and source fields are both key, which means each record's re-source combination must be unique.Typically, you see no more than two records with the same re, and only if:

- One RE is has a regular source (NFM, CP, etc.). CIMs are regular.
- One RE is has a GeoProbe source. CIMs are CDRs.

referral Table

Purpose

This table is used by network managers (normally NOT by system administrators) to keep track of problem referrals.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
refer-ral	ne	clli, scpclli, ne, adjclli, or area	swarch, scparch, stparch, adjarch or ecosarch
	fdc	fdc	fdc

reports Table

Purpose

The reports table defines customized reports that are accessible remotely (from the BB-GUI). It specifies:

- The name of the report.
- What command will run the report.
- The number of rows and columns in the report.
- Helptext to be displayed in the report.

It also allows the report to be restricted to members of a specified FDC groups.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
reports	fdcgroup	name	fdcgroup

route1a Table

Purpose

Use this if you have 1A ESS RE's. This table identifies distant entities for each reporting 1A ESS entity. The 1AESS route (route1a) table associates 1A ESS trunk groups with Distant Entities in order to support the 1A ESS switches as reporting entities (RE's).

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
route1a	clli	re	rearch
	de	clli	swarch

route5e Table

Purpose

Maps an RE to its Des. Use if an RE is:

- 5ESS
- 7R/E PLS
- (5ESS) AUTOPLEX MSC

For CFIMs from 5ESS switches (and other RE types that use the Route5e table, NTP uses this table to find the RE's DE. Specifically, NTP looks in this table for the RE's CLLI and the CFIM's Tgn, and takes the corresponding DE.

Important! Switching the Trunk Group Suffix feature on enables the user to identify trunk groups more easily, because of the suffix field (sfx) that is added to the cfim record. For more information on the Trunk Group Suffix feature, see Chapter 5 "Trunk Group Suffix (Sfx)" (p. 4-58).

Field dependency

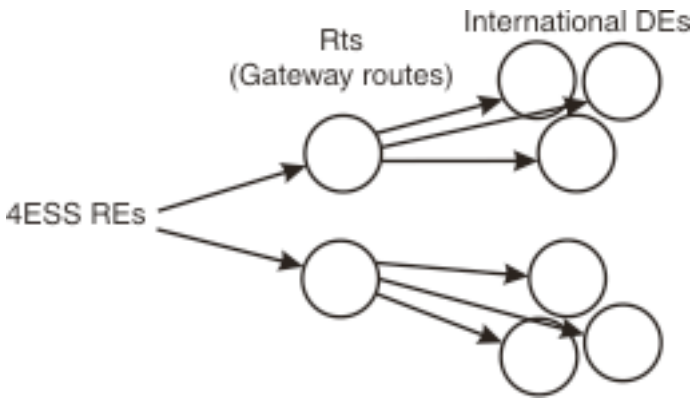
In table...	Before you put a value in field...	That value must be in field...	In table...
route5e	clli	re	rearch
	de	clli	swarch

rtarch Table

Purpose

Use this if you have 4ESS REs, monitoring Rts (country gateway route).

An Rt is a field on CFIMs. This table names international gateway routes (Rts) so they can be mapped to DEs in the de2route table. Rt-to-DE routing is illustrated below.



Rtarch and De2route tables define the Rt field for 4ESS switches only. (Softswitch also populates the Rt field, on CFIMs, but does NOT use Rtarch and De2route tables.)

Field dependency

Reference: Updating this table is explained at "Add an Rt" (p. 4-56).

s1240route Table

Purpose

This table identifies distant entities for each Alcatel S1240 RE. The S1240 route table shows how other switches are connected to your S1240 switches. When NTP receives a CIM from an S1240 RE, NTP reads it to get the trunk group used, and then uses this table to determine the DE. NTP then puts that DE in the DE field of the CFIM it create from the CIM. (Otherwise, the DE field will say "?".)

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
s1240route	clli	re	rearch
	de	clli	swarch

scode2sig Table

Purpose

Use if you have RE's from AXE 10. Derives CFIM's signaling type (sig field) from Arbor BP call detail record (CDR) CIMs.

This is one of four tables (dcode2d, scode2sig, stcode2st, id2ne) dedicated to telling how to translate Arbor BP CIMs to CFIMs. The fdc and acode2fdc tables are also used.

Reference: See Step 13 in "Add or modify an FDC" (p. 4-78) for when this table is used.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
scode2sig	signaling	type	signal-ing

scparch Table

Purpose

Use this if you have 4ESS or DMS Retypes. The SCP architecture (scparch) table enables NTP to correctly fill in CFIM Rs and Ds fields, and enable's SCPs to be RE's.

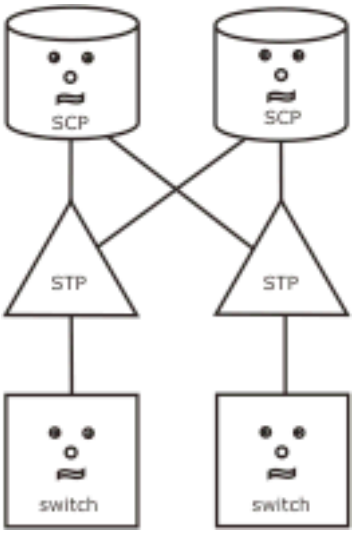
Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
scparch	stp	ne	stparch

scproute Table

Purpose

Use this if you have 4ESS or DMS RE's. The SCP route (scproute) table maps digits to SCPs, so NTP can identify SCPs as DE's to 4ESS or DMS RE's. An SCP is actually a pair of databases, used by a pair of STPs (signal transfer points), which supply signalling (SS7) data to network elements such as switches.



Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
scproute	scpclli	scpclli	scparch
	signet	name	signet

Note

SNAP. With 4ESS switches, if you have access to SNAP (signaling network architecture platform, formerly called CINTAS), you can have SNAP send you periodic updates, in the form of 3 and 6-digit GTRK mapping data. Once you receive this SNAP data, run this script to use the data to update 4ESS entries in scproute:

```
$APPLBIN/Snap input_filename
```

You can also run this script from cron. In $LOGDATA, updates are logged in snlog and errors in snerr.

sdthresh Table

Purpose

The system day threshold (sdthresh) table contains individual system day thresholds overriding the system day default threshold. Putting an RE or FDC in this table does NOT cause it to use system day thresholding (in place of normal 5-minute and hourly thresholding). To do that, you would go to the FDC table and put d in the tm field. Then, if you want to set system day thresholds for the FDC (in place of the default system day threshold), use this table.

Important! This table is used only if system day thresholding is activated for your system.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
sdthresh	fdc	fdc	fdc
	ne	clli, scpclli, ne, adjclli, or area	swarch, scparch, stparch, adjarch, or ecosarch

sgsn_ref_data Table

Purpose

The sgsn_ref_data table defines SGSN components in the UMTS network and their relationship to a packet core network.

Field dependencies

In table...	Before you put a value in field...	That value must be in field...	In table...
sgsn_ref_ data	sgsn	clli	swarch
		re	rearch
	pkt_core_id	pkt_core_id	pkt_core_ref_ data

sdttype Table

Purpose

Use if you have 4ESS RE's.The segmentation directory transition type table (sdttype) translates a CIM's 1- or 2-digit SDTT ID code into the CFIMs10-character sdtt name.

Example: One customer is moving call routing and servicing from 4ESS switches to a separate processor. There calls are routed or serviced using the Segmentation Directory (SD). On 4ESS CIMs, a 1- or 2-digit code labelled SDTT (Segmentation Directory Transition Type) identifies the routing or servicing the SD did for the call. On 4ESS CFIMs, instead of a 1- or 2-digit SD code, NTP gives a name in a 4-character field named sdtt. If users need an explanation for an sdtt, they can look up its description in the sdttype table.

Services under (or scheduled to be under) SDTT include:

- SDN — Software defined network
- USDS — Universal subscriber data structure
- POTS — Plain old telephone service
- PCPC — Positive call processing cellular
- SDS — Switched digital services
- iPCC — True Voice ANI indicator controlling True Voice ANI individual per Call Control (formerly in the 4ESS switch ANI trigger table)
- CSRO — True Voice ANI indicator controlling Customer Specific Routing Option for switched access direct customers (formerly in the 4ESS switch ANI trigger table)
- DL — 1+Directory Link Blocking indicator for directory assistance calls (formerly in the 4ESS switch ANI trigger table)
- QuiteHear indicator for 1-800-ATT calls (formerly in the 4ESS switch ANI trigger table)
- CPPA — Calling party pays airtime indicator for EasyReach 500 calls (formerly in the 4ESS switch ANI trigger table)

Field dependency

None.

searchalias Table

Purpose

The search alias (searchalias) table lists the 4-character aliases for the network entities (except STPs). Network administrators can use aliases in place of CLLIs.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
sear-chalias	ne	"clli" type fields (this has different names in the tables at right)	swarch, scparch, ecosarch, or adjarch

sensor2clli Table

Purpose

The sensor2clli table translates sensor ids to clli codes for use in populating re values.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
sensor2clli	clli	cllli	swarch

sigdigpp Table

Purpose

The sigdig table allows you to do a significant digit analysis on data by defining different significant digit patterns.

The digits and cpdigits are divided based on NPA-NXX-XXXX format. You can enter up to 4 different patterns for any of the digit type fields found in the cfim table.

After these fields are defined in the sigdig table, you can then access them as you would any other cfim table fields by using the Properties->Data tab option from the Parabox and Piechart displays.

Important! This table affects Pattern Painter only. Pattern Painter runs in association with the BB-GUI.

Default Entries

The sigdig table contains two default entries. These entries analyze the DIGITS and CPDIGITS values using the NPA and NXX patterns.

```
#Fieldname|Sigfield1|Siglen1|Sigfield2|Siglen2|Sigfield3|Siglen3|Sigfield4|Sigle
   n4
digits|dig_npa|3|dig_nxx|6|-|-|-|-
cpdigits|cpdig_npa|3|cpdig_nxx|6|-|-|-|-
```

With these two default entries, the Parabox display will show different columns for the DIG_NPA and DIG_NXX values as being the first 3 or first 6 characters of the DIGITS string.This allows for better analysis of a network problem.

Additional Entries

Dbedit the sigdig table to add fields to the table. This example shows a field added for billdigits.

```
#Fieldname|Sigfield1|Siglen1|Sigfield2|Siglen2|Sigfield3|Siglen3|Sigfield4|Sigle
   n4
digits|dig_npa|3|dig_nxx|6|-|-|-|-
cpdigits|cpdig_npa|3|cpdig_nxx|6|-|-|-|-
billdigits|billdig_npa|3|billdig_10|10|-|-|-|-
```

The Parabox display will now show different columns for the billdig_npa and billdig_10 values as being the first 3 or first 10 characters of the billdigits string.

The values used in fieldname should be one of the valid digits type fields already defined in the cfim table. Those digit type fields are:

- cpdigits
- digits
- billdigits
- dsdigits
- servdig
- lrn
- psn

Field dependency

There are no fields in this table whose values must be defined in other tables.

signaling Table

Purpose

You may edit this when you implement any conversion (1AESS, 4ESS, IPDR, etc.), since when you add a new Retype, you also add its FDCs, and you can map any FDC to a signalling type—in the FDC table's sig field—and what you put in that field must first be defined here. What you put int that field is output to the signaling field of any CFIM with the FDC.

Signaling types must be defined here in the type field before they can be used in the:

- dmsroute table's sig field
- ess1a2fdc table's sig field
- fdc table's sig field
- scode2sig table's signalling field
- univroute table's sig field

This table is populated with standard signaling types at installation.

Field dependency

None.

signet Table

Purpose

Use this if you use the multiple signaling networks feature to identify SCPs as DE's although they are in different signaling networks.

Signaling networks must be defined in the name field here before they can be used in the signet field in these tables:

- stparch
- adjroute

Without this feature, determining SCP-DE's can be problematic, since calls with the same digit string may have different translations and may be routed to different SCPs, depending on which network is the location of the originating Service Switching Point (SSP).

For example, an 800 number that can be called by customers in two signaling networks may be translated by a different SCP pair, depending on where the call originates. NTP can determine the correct SCP pair by identifying the signaling network of the originating call in the stparch table, and using that as a key for a lookup in a routing table. This feature is necessary if the same translation may be performed by different SCPs—that is, if NTP is monitoring more than one signalling network (including disaster recovery schemes in which NTP monitors a secondary network).

If you do not use this feature, still leave the preloaded values in the table. This table can have up to 4 records, for 4 supported networks.

Field dependency

None.

siptg_reference Table

Purpose

This table is associated with SIP Trunk Groups. For example, in Lucent Plexus Network Controllers, such trunk groups run from Media Gateway Controllers to Feature Servers (or other SIP Signaling servers like the Lucent Session Manager).

source Table

Purpose

The source table names and identifies the CIM sources (collectors, interfaces) connected to NTP through which NTP receives data for RE's. Sources include element management systems, mediation systems, and direct interfaces.

Field dependency

- For customers who do NOT use RDS (reference data synchronization— refsynch), there are NO field dependencies.

For customers who DO use RDS, the following field dependency applies for this table.

In table...	Before you put a value in field...	That value must be in field...	In table...
source	name	name	bdrhost

Note

- RDS. This table is NOT synchronized by refsynch (see "What data is synchronized for RDS?" (p. 12-2)).
- Sources and converters. For interfaces requiring specialized converters, the value in the type field in this table may resemble the value in the conv field in the "rearch Table" (p. A-129), and this can lead to confusion. The type field here designates the type of source from which NTP receives data and NOT the software module (converter) NTP uses to convert CIMs to CFIMs.
- One source per RE. For some interfaces you must add a SEPARATE source for EACH RE. This is because NTP cannot identify the RE without relating it to a unique source.
  - Direct OTR TOPS or OSPS interface (For OTR interfaces through an EMS such as NFM, multiple RE's can use the same source.)
  - Succession SN05 and SN06 interface
  - Some custom interfaces (typically direct)

  Reference: For information on which RE's can use which source types, see "Source Types and REs" (p. 5-10).

source_procs Table

Purpose

This table defines additional processes that need to be launched for a particular process. This table is used for the SIP Log conversion. In the case of SIP Log, for each instance, an entry needs to be added that contains the source name, and the command line arguments that are required to start **ssh** for that source.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
source_ procs	source	name	source

st Table

Purpose

This table defines service types known to NTP. A service type must be defined here before it can be used in the fdc, gtspec, domain, cos (class of service) or stcode2st table. This table is used for the following conversions:

- EWSD
- GeoProbe
- AXE 10 (Arbor BP)
- AXE 10 TRADO
- Lucent Softswitch

IPDRs

Field dependency

None.

ss7link_reference Table

Purpose

The SS7 Link Reference Data table includes reference data associated with SS7 Links.

stcode2st Table

Purpose

This table derives a CFIM's service type (st field) from CDRs or IPDRs. This table is used for the following conversions:

- AXE 10 (This is one of six tables [fdc, acode2fdc, dcode2d, scode2sig, stcode2st, id2ne] that translate Arbor BP CIMs to CFIMs.)
- AXE 10 TRADO
- Lucent Softswitch
- IPDR

  Reference: See Step 13 in "Add or modify an FDC" (p. 4-78) for when this table is used.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
stcode2st	st	type	st

std_dig_list

Purpose

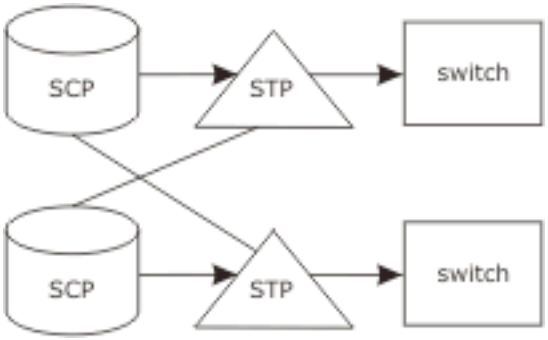
This table is used with the optional Digit Standardization feature.

The std_dig_list table contains a list of special digit strings.

stparch Table

Purpose

Populate this table so that you will see values in the CLLI fields Rs and Ds.



The STP architecture (stparch) table maps an STP ID to the CLLI code of each STP pair. The record includes the ID for the hierarchical STP pair, the signaling network the STP is in, and the owner of the STP. An STP pair must be defined by a record in stparch before it can be used in the stp field of a swarch record (note that both members of the pair are defined by one record).

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
stparch	owner	id	owner
	signet	name	signet

Important! The ne field must contain a unique value which is not defined in a field in one of the following tables:

- swarch.clli
- adjarch.adjclli
- lrarch.clli
- rtarch.rt
- ecosarch.area

swarch Table

Purpose

The switch architecture (swarch) table defines all REs known to the system, and most DEs (see “"Arch" and route tables” (p. 4-7) for full details).

Important! OTR TOPS DMS "fake" CLLI's. For OTR TOPS modules on DMS switches as RE's, if you already added to swarch the DMS switch on which a TOPS module resides, then add the TOPS module with a fake value in the clli field.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
swarch	clli (See AXE10 note, above.)		
	eqtype	type	eqtype
	stp	ne	stparch
	owner	id	owner
	ccd	ccd	country

Important! The clli field must contain a unique value which is not defined in a field in one of the following tables:

- stparch.ne
- adjarch.adjclli
- lrarch.clli
- rtarch.rt
- ecosarch.area

sysuser Table

Purpose

The system user (sysuser) table lists NTP users. It is populated when NTP users are added or deleted (see "add_ntpuser Command" (p. 6-25) and "del_ntpuser Command" (p. 6-32)).

Important! The following fields do NOT affect the BB-GUI. They do, however, affect the SUI: cmdgroup, fdcgroup, netgroup, restricted. For affected users, this table is modified by the "mod_cmdgrp command" (p. 7-14), "mod_fdcgrp command" (p. 7-24), and "mod_netgrp command" (p. 7-43). The equivalent attributes (except command groups) are set SEPARATELY for the BB-GUI.

Field dependency

n able...	Before you put a value in field...	That value must be in field...	In table...
sysuser	cmdgroup	name	cmdgroup
	fdcgroup	name	fdcgroup

tcapdiag Table

Purpose

The tcapdiag table contains a textual mapping of the hexadecimal error code found in the TCAP message to a text string that will be placed in the CFIM.

Field dependency

None.

tg_reference table

Purpose

The Trunk Group Reference Data table includes reference data associated with SS7, BICC, and CAS Trunk Groups. Trunk Group data is only reported from the Media Gateway Controller viewpoint.

thresholds

Purpose

The thresholds table shows threshold status and current values for each entity, FDC and load set period ID (LSPID).

Field dependency

None.

tst_num_std_rule

Purpose

This table is used with the optional Digit Standardization feature.

The tst_num_std_rule table contains test rules used by the digit standardization testing tool. The rules indicate how to standardize a digit string and how to determine customer type.

tst_patrn2rule

Purpose

This table is used with the optional Digit Standardization feature.

The tst_patrn2rule table contains test "patterns" that are used by the digits standardization testing tool to check user supplied data and determine which entry in tst_num_std_rule to execute. Checks may be performed on called and calling party digit lengths, called and calling party contents, and trunk group information. All defined checks executed and if they are all successful the appropriate rule in tst_num_std_rule is executed and the resulting values are output by the test tool.

univconfig Table

Purpose

The universal interface link configuration (univconfig) table enables the system administrator to custom-configure conversions.

Background

Delimiter characters (SOM and EOM) are a decimal representation for the delimiter byte. For example, a ^B in UCIMs is an ASCII translation of the start of text character, which is specified by its decimal value of 2.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
univconfig	source	name	source

univroute Table

Purpose

The universal route (univroute) table identifies distant entities for RE's by associating switch and trunk group information with a distant entity (DE).

Important! Switching the Trunk Group Suffix feature on enables the user to identify trunk groups more easily, because of the suffix field (sfx) that is added to the cfim record. For more information on the Trunk Group Suffix feature, see Chapter 5 "Trunk Group Suffix (Sfx)" (p. 4-58).

Reference

This table is used for all converters using the Configurable Conversion (see Chapter 13, "CIM Source Administration", section "Overview of Sources for Configurable Conversions" (p. 5-40)).

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
univroute	clli	re clli	rearch swarch
	de	clli	swarch
	sig	type	signaling

utran_ref_data Table

Purpose

The utran_ref_data table is used to define a unique UTRAN identifier. It can be used to create a set of logical UTRAN networks based on regions and associate components that are within that region with the logical group.

vpnid Table

Purpose

Not yet used for standard conversions, but available for CDR-type installations.

The virtual private network ID (vpnid) table contains each VPN customer name and telephone number. It is nice to see the customer's name in the CFIM's Cust field, but the name is not on CIMs. But CIMs give other information, which you can map to a name to populate the Cust field by using the following tables (different conversions use different sets of these tables):

- "custcode Table" (p. A-50) — Use this if you get REDE's from IPDRs. Maps a customer name to an account code, subscriber id, or other unique identifier. Populates the Cpcust and Cust fields on CFIMs.
- "custid Table" (p. A-51) — Maps each IDB/DSD or other non-VPN customer's name to a phone number. If no match is found, the CFIM's Cpdigit's value is placed in Cust.
- "vpnid Table" (p. A-166) — Maps each VPN customer's name to a VPN. If no match is found, the VPN is placed in Cust.
- "custip Table" (p. A-52) — Maps each customer's name to an IP address.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
vpnid	custname	cust	customer

vpnroute Table

Purpose

Not yet used for standard conversions, but available for CDR-type installations.

The virtual private network route (vpnroute) table contains the VPN routing numbers and their corresponding DSD/SCP pairs information. It lists the originating NPAs for VPN customers and their associated DSD/SCP IDs where the VPN calls are routed.

Field dependency

In table...	Before you put a value in field...	That value must be in field...	In table...
vpnroute	scpclli	scpclli	scparch
	signet	name	signet

Appendix B: SUI Commands

Overview

Purpose

SUI (shell user interface) commands are Network Trouble Patterning software commands entered from the operating system shell, preceded by **`sui`**.

Example: To quickly see Alert Cases output, you can enter **`sui ascreen`** directly from the shell, without starting up the GUI.

This chapter discusses general information about sui commands as well as detailed information about each command. Procedures for working with variables are also found in this chapter.

Contents

Introduction

Why type "sui"?

Some NTP commands, such as **sort** or **help**, may be named the same as existing operating system commands. To specify the NTP command, you must precede it by **sui**.

Hint: When in doubt, precede a command with **sui**. *If that fails, drop the* **sui**.

SUI output

If a SUI command gives output, the output appears in the window where you executed the command.

Summary of SUI Commands

List of SUI commands

This table summarizes the function of SUI commands described more fully in this and other chapters of this book.

Command	Purpose	Reference
sui acresolve	(Alert case resolve) Searches for active alert case records that satisfy specific criteria,	"sui acresolve Command" (p. B-9)
sui ascreen	Runs Ascreen in an X window	"sui ascreen Command" (p. B-14)
sui compute	Runs Ascreen in an X window.	"sui compute Command" (p. B-16)
sui find	Retrieves records from databases. Use with **dbedit**.	"sui find Command" (p. B-18)
sui help	Explains FDCs.	"sui help Command" (p. B-34)
sui join	Joins two user files (databases) into one.	"sui join Command" (p. B-35)
sui linkmon	Allows daily monitoring of the links between reporting entities (switches) and sources.	"Syntax for dbedit" (p. B-20)
sui list	Lists all user files (databases) belonging to your own login.	"sui list Command" (p. B-40)
sui remove	Removes your user databases (user files). With **force**, removes others' user databases.	"sui remove Command" (p. B-42)
sui rename	Renames user files (databases).	"sui rename Command" (p. B-44)
sui set	Sets an environmental variable (such as default printer) for your own login. (By convention on *UNIX* systems, environmental variable names are in capital letters.)	"sui set Command" (p. B-45)
sui setsys	Sets thresholding variables.	"sui setsys Command" (p. B-50)
sui sort	Sorts the records in a user database file.	"sui sort Command" (p. B-51)
sui trapalert	Runs Trapalert in an X window.	"sui trapalert Command" (p. B-52)

Command	Purpose	Reference
sui trapcfim	Runs Trapcfim in an X window.	"sui trapcfim Command" (p. B-53)
sui trapdata	Runs Trapdata in an X window.	"sui trapdata Command" (p. B-54)

Syntax

Purpose

This section provides general information about SUI command syntax. See each command in this tab for its specific syntax.

Syntax elements

A SUI command such as **`sui find source=cfim search=fdc=nca`** has the following syntax:

```
command     parameter=value
   parameter=subparameter     operator     value
```

Syntax elements include the following:

Element	Purpose	Example
command	Tells what to do	**`sui find source=cfim search=fdc= nca and tc!=dms`**
parameter	Affects a command. Always followed by =*subparameter* or an operator value.	**`sui find source=cfim search=fdc= nca and tc!=dms`** For how to use the search parameter, see the *BB-GUI User's Guide*.
subparameter	Limits a parameter. It is a tablename, field name, or other defined set of values. Preceded by a *parameter*= and followed by an operator value.	**`sui find source=cfim search=fdc= nca and tc!=dms`**
operator	=, !=, <, >, <=, >= (precedes a value)	**`sui find source=cfim search=fdc= nca and tc!=dms`**
value	Follows an operator	**`sui find source=cfim search=fdc= nca and tc!=dms`**
Boolean	and, or	**`sui find source=cfim search=fdc= nca and tc!=dms`**

Command and parameter abbreviation

You need type only enough to uniquely identify a command or parameter.

Example: Instead of: **`sui find source=cfim search=fdc=942`** You can type: **`sui f so=cfim se=fdc=942`**

Spaces in Search Expressions

If a search expression item contains a space, that item must be enclosed in double quotes and the quotes must be escaped with the backslash character. Otherwise, the sui will generate an error.

Example:

Incorrect:

```
sui find so=acode2fdc se=acode="cell failure" and fdc=celfail
```

Correct:

```
sui find so=acode2fdc se=acode=/"cell failure/" and fdc=celfail
```

Parameter order

Parameters can be in any order.

Example: **`Example: sui find source=cfim search=fdc=nca`** and **`tc!=dmssui find search=tc!=dms`** and **`fdc=nca source=cfim`**

Parameter values

About parameter values:

- **`Multiple.`** Multiple values can be assigned to a parameter, separated by commas, for example:

  Example: **`sui find source=cfim search=fdc=nca,vca,1987`**
- **`search`**=. For how to use search parameters, see the *BB-GUI User's Guide*.
- **`Types`**. Parameter values are of four types:
  - **`Time`** - Use HHMM or HH:MM (for example, 1349, 13:49, 6:49, 06:49).
  - **`Date`** - Use YYMMDD, MMDD, or YY/MM/DD (for example, 941221, 1221, 94/12/21, 94/6/30).
  - **`Numeric`** - Whole numbers with the digits 0 to 9. (Exception: The *min* parameter in compute can contain a decimal point.)
  - **`String`** - Valid characters for a string are *A* to *Z, a* to *z, _, 0* to *9, ., /*, and *!*. Strings can use other characters and spaces IF the string is enclosed in double quotes, and then single quotes.
- **`Wildcards`**. A string parameter value can use * or *&:*
  - * means any number of characters.

    Example: **`sui find source=swarch se=clli=5*tz*`**
  - & means single characters:

    `Example: sui find source=swarch se=clli=&&&&ny&&&&`

User variables

User variables are string substitutions (explained in the *BB-GUI User's Guide* and "sui set Command" (p. B-45)). All or part of a SUI command can be a variable. When used, variables must be preceded by "$", and surrounded by SINGLE quotation marks. For example: sui '$myfindf1' or sui find se='$mysearch'

Operators

Operators are:

Operator	Means	Use with this parameter type
=	equal to	Any
!=	not equal to	
>	greater than	Numeric only
<	less than	
>=	greater than or equal to	
<=	less than or equal to	

Boolean

Booleans are:

Boolean	Means
and	include records that agree with BOTH parameters.
or	include records that agree with EITHER parameter.
and not	include records that BOTH: agree with the previous parameter, and NOT the next.
or not	include records that EITHER: agree with the previous parameter, or NOT the next parameter

Output to file

To send a SUI command's output to an ASCII file, use a redirect (>), as you would with any shell command.

Example: To send output to a file named tempfile enter

```
sui find source=swarch search=ne=12345 > tempfile
```

sui acresolve Command

Description

The sui acresolve (alert case resolve) command displays active alert case records that satisfy search expressions you specify. You can also:

- View or trap CFIMs related to those alert case records
- Update alert case records with problem resolution information by specifying a value in one or more of the following fields:
  - owner
  - referred
  - status
  - fcause (failure or event cause)
  - comments
- Group alert case records for the same problem by assigning the same trouble number, or ungroup previously grouped records
- Close one or more alert case records

Syntax

```
acresolve search= [not] field=value1... and/or [not]
   field=value1,value2...
   owner=value referred=value status=value fcause=value
   comments=text dest=value save=user_file_name group=g/u view
   trap
```

When you specify a value for any parameter in addition to the required search parameter, NTP modifies all the records that satisfy the search, displays the CFIMs (if directed to by viewcfim=y) and completes command execution.

When you run acresolve and specify only the required search parameter, NTP displays the resulting records.

Parameter	Description
Search (required)	Specifies the criteria to select and display records. Maximum length: 1500 characters. Valid characters for the owner, referred, fcause, and comments fields are: *A* to *Z, a* to *z, _, 0* to *9, ., /*, and *!* Enclose printable characters other than the above in double quotes (for example, *owner="Joe,Mary"*). These fields do not allow the **, $*, or *&* characters except as part of a search expression. Please note the following: The FDC_SEARCH variable setting controls the default set of FDCs that are searched when you do not specify a list of FDCs. • **group** — Searches only records with FDCs valid for your current FDC group. • **all** — Searches all records. The NET_SEARCH variable setting controls the default set of network entities that are searched when you do not specify a list of NEs. • **group** — Searches only records with entities valid for your network segment group. • **all** — Searches all records. You can specify a TN in your search that involves an FDC or NE not in your FDC or network segment group, but the corresponding _SEARCH is set to **group** as opposed to **all**, you will not retrieve the record. Add the affected FDC or NE to the search expression so the _SEARCH setting is ignored. Restricted users see only FDCs or NEs in their group regardless of the FDC_SEARCH or NET_SEARCH setting or the search expression. *Reference* • See "User environment variable list (admset)" (p. 7-50) for more information on the FDC_SEARCH and NET_SEARCH variables. • See "Search Expressions in sui find" (p. B-29), for examples of search expressions.
Owner (optional)	Name of the person or organization (up to ten characters) to which the case is assigned for resolution. Default value: -.
Referred (optional)	Name of the person or organization (up to ten characters) to which the case is referred for resolution (for example, the owner of the case may have a call in to the organization listed in this field). Default value: -.

Parameter	Description
Status (optional)	Status of the case. Values: • Enter **closed** in this field to close the alert case record and make it inactive. (Once an alert case record is inactive, you cannot use **acresolve** to subsequently display or modify it. You can view inactive alert case records via the **find acase** command.) • If there are no values in the referred or owner fields, the system lists the status as **open**. • The system automatically changes status to **assigned** or **referred** (in that order) when you enter a value in either of these fields. The system can also automatically close a case record when conditions set by the NTP administrator are met and the current status is not **referred**.
fcause (optional)	Identifies the cause of a failure or event. Causes are customer-defined (see "fcause Table" (p. A-67)). You must enter an exact value of a cause defined for your system.
comments (optional)	Contains user comments detailing the problem or resolution. You can enter a continuous string or the ^ character to represent a line return. To enter: • a single word comment (no spaces), use double quotes. *Example:* **comments="Translations"** • a multiple word comment (with spaces) – use double quotes enclosed in single quotes. *Example:* **comments='"Install new translations at switch. Stripping instructions incorrect"'** – use the ^ key to denote a page break every 76 characters. There is a maximum length of 308 characters in a comment. *Example:* **comments='"Install new translations at switch. Stripping instructions incorrect. See^ System Administrator for further information."'**
save (optional)	Specifies a file name in which to store CFIM records that result from a View CFIM. Length: up to 30 case-insensitive characters. The name must begin with an alpha character and consist of alphanumeric and underscore characters only. Default: Leave this field blank to store records in the default file ws_view. The ws_view file is overwritten with each execution of the View CFIM function. A most recent backup copy is named ws_view_prev.

Parameter	Description
destination (optional)	Where CFIM output displays when View CFIM is selected. Valid destinations are: • **pager**, or blank (default) — Your terminal screen via the standard pager. • The name of a printer on your system or lp (defaults to the printer defined in the PRINTER environment variable.) • **lplocal** — A printer attached to a 630/730 terminal. You can also use lplocal if you logged in as an xterm and your system has optional local printer support for xterms. • *filename* — Name of an ASCII file. • **terminal** — Your terminal screen, bypassing the standard pager (useful if you are running on a PC or wish to send to an unsupported local printer). • **null** — No output display. Selected records are stored in ws or a named user file.
group (optional)	Values: • **g** (group) — Groups all the alert cases in the current set and assigns the lowest TN of the group as the TN for each record of the group. (Grouped records are all assigned the same trouble number so you can track the problem and search for records by that one number.) • **u** (ungroup) — Ungroups the alert case records and returns the TN back to the ACN of the record. Each alert case record is assigned an alert case number (ACN) and trouble number (TN). ACNs are assigned sequentially for each alert case. If you have the trouble number grouping feature turned on, alert cases for the same FDC that began alerting at the same time are assigned the same TN, which is the first ACN of the group. Thus, you can track the same problem by TN. See information on the Acase table in the *BB-GUI User's Guide*.
viewcfim (optional)	Value: **view** — Indicates that you want to view the CFIMs related to the alert cases that satisfy your search. The related CFIMs are in a user file called ws_view.
trapcfim (optional)	Value: **trap** — Indicates that you want to trap the CFIMs related to the alert cases which satisfy your search. The incoming CFIMS will display in a Trap Data window as they generate. The output format for trapped CFIMs is determined by your CFIM_FORM variable, if one is set, or by the system default. See "User environment variable list (admset)" (p. 7-50) for more information.

Examples

The following examples illustrate various uses of acresolve.

Purpose	Command
Search and do batch edit	This command finds all alert case records that have trouble number (Tn) of 7 (search field), and adds the same failure or event cause to the fcause comment field for ALL records found. **acresolve search=tn=7 fcause=install comments= "Install of new translations at the switch^ Stripping instructions incorrect"** The ^ indicates a new line in the comments field.
Trap related CFIMs	This command traps all CFIMs that have trouble number (TN) of 8. **acresolve search=tn=8 trap**
Group alert case records by TN	This command groups CFIMs that have trouble number (TN) of 7, 9, or 10. **acresolve search=tn=7,9,10 group=g**

sui ascreen Command

Purpose

The **sui ascreen** command shows active alert cases. Ascreen automatically updates periodically. To exit, press **Delete**.

Important! The Alert Cases page shows the most recent alert cases. However, if both a 5-minute and an hourly alert case are open at the same time, the 5-minute alert takes precedence, and the hourly alert is not shown. This is true even if the 5-minute alert has a negative CAI (current alert interval) and the hourly alert has a positive CAI.

Reference: For how to read Ascreen, see the *BB-GUI User's Guide*.

Syntax

```
ascreen search= [not] field=value1... and/or [not]
field=value1,value2...
sort=field1:a/d,field2:a/d . . .
format=field1,field2:width,field3,...
fdcgroup=all/group_name netgroup=all/group_name
```

Important! These parameters apply one time when entered. To permanently change a parameter for your login, use the admset command on your environment variables (see "Reprocess CDRs" (p. 10-42)), or you can do the same by customizing (see the *BB-GUI User's Guide*).

Parameter	Description
Search (optional)	Selects which alert cases appear on Ascreen. Omit to see all. Reference: For how to build search expressions, see the *BB-GUI User's Guide*.
Sort (optional)	Gives output sort. List fields in the order you want them processed, with "a" for ascending sort or "d" for descending sort. *Example:* **sui sort=cai5:d,cnt5:d**
format (optional)	Selects output screen format. Options are: • Enter **all** to display all the fields. • Enter a list of field names separated by commas in the order you want. *Example:* **format=fdate,ftime,ldate:5,ltime, ne,type,fdc,tc,tn, cnt5,cai5,cnth,caih,owner** • To change field size, follow the field name with colon and number of characters. *Example:* **format=fdate:5,ltime:5, ne:16**

Parameter	Description
fdcgroup (optional)	Limit output according to an FDC group. Options are: • **all** • An FDC group name To list FDC groups, see "List FDC groups" (p. 7-18).
netgroup (optional)	Applicable only if you have the optional network grouping feature. Limit output according to an network group or segment. Options are: • **all** • A network group name To list network groups, see "List network segments and groups" (p. 7-33).

Example

```
sui ascreen
```

sui compute Command

Purpose

The sui compute command looks for patterns in groups of records.

Reference:

- For how to read Compute, see the *BB-GUI User's Guide*.
- For how to use the sui set command to define the ASCREEN_FORM variable or your own named FORM variable, see"sui set Command" (p. B-45).

Syntax

```
compute file=userfile row=field1,field2,...fieldN
cololumn=fieldname=value1,value2,...value12 output=count or
percent min=value title="title" sort=count or value
intnterval=time interval
```

Important! These parameters apply one time when entered. To permanently change a parameter for your login, use the admset command on your environment variables (see "Reprocess CDRs" (p. 10-42)), or you can do the same by customizing (see the *BB-GUI User's Guide*).

Parameter	Description
file (optional)	Selects the user file (database) to compute on. If omitted, the working set (ws) is used. Non-restricted users can use another user's file by including the user ID followed by a slash prior to the file name (for example, **sjm/rpt94**).
row (required)	Selects at least one row to sort on. Separate multiple rows with commas; no spaces. *Example:* **row=fdc,de**
column (optional)	Selects one or no columns to sub-sort on. Can also limit output according to matches you give. *Example:* **column=re** **column=(re=switchaus01t,switchb02t)**
output (optional)	• To label output as counts, use **output=count** This option can be used only when both row AND **column** are desigated. • To label output as percentages, use **output=percent** This affects the min parameter. For example, if you set min=2, the output parameter determines whether to compute on a minimum of count 2 or 2%.

Parameter	Description
min (optional)	The lowest numerical value to appear on compute output. Values for **min** can be a whole number in the range 0 to number of records minus 1, or a percent in the range 0.00% to 99.99%. If omitted, default is1 or .01% *Example:* To display compute output for only those digit patterns that appear at least 100 times in the user file, enter **row=digits,min=100** When you use the column field, the sum of the columns beside any row value will be >= min count, even though individual column cells for a row value may be < than min count.)
title (optional)	Title you want to appear on output. Up to 80 characters. Enclose in double quotes, and then single quotes. *Example:* **title='"OCT. - NOV. RESULTS"'**
sort (optional)	To sort row values: • Biggest to smallest (default), enter **sort=count** • Alphanumerically, enter **sort=value** If you specify a column, sorting is always by value.
interval (optional)	Selects a time interval displayed on the output. You can use this only if a row is a time-related field. If omitted, defaults to 1 minute. Enter interval as *nn* **min** or *nn* **hour**, where *nn* can be any integer from 1 to 59 (min) or 1 to 23 (hour). *Example:* **interval=10min**
delim (optional)	Defines a single character that the database editor is to interpret as the delimiter of fields in an input record line. (**delim='";"** replaces blanks between fields with semi-colons, to avoid confusion when you later dbedit the data.) *Example:* **sui compute row=time sortby=value interval=time:5min delim='";"**

Example

```
sui compute row=digits,de title="Compute Digits" min=50
```

sui find Command

sui find purpose

The sui find command retrieves data from databases. When you retrieve that data, you can either:

- Save the data into an ASCII file for further use
- View the data on your screen, to check it

ASCII files saved from sui find are most often used as input with the dbedit command, which modifies NTP database tables (see "Dbedit" (p. 3-17)). Many procedures in this book require dbedit. You can also print the ASCII files, or email them to someone.

After a dbedit operation, sui find can help you verify that you have indeed made the changes you want to the NTP reference database.

Important! The sui find command is most often used when working with Reference Database tables. See Chapter 3, "Reference Data Tables" for more information.

Command syntax

```
sui find source=user or system file
 save=user_filename
    search=field=value1,value2
... and/or [not] field=value1
    format=field1,field2:width,field3
... dest=destination
    rangange=n to maxsave-1 (range cannot exceed 30,000)
    maxsave=n (n can be 0-100,000)
 fdcgroup=
    netgroup= findtime= netsearch= fdcsearch=
    delim='"delimiter
"' noheader
```

Note: To filter the results using either netgroup or fdcgroup, use parameter netsearch or fdcsearch, respectively.

The parameters associated with sui find are detailed in the next section (see "sui find for dbedit" (p. B-20)).

Basic sui find

The simplest case for using sui find is to send the all records from a database to your screen, by entering: sui find source=database

To see the contents of the fcause database, enter sui find source=fcause

Output goes to your screen, resembling this:

```
Reason     Description
FIND COMPLETED - 5 FCAUSE RECORDS FOUND
install    Installation related
routing    Network routing error
translate  Digits translation error
testing    Network testing related
unknown    Failure reason unknown
FIND COMPLETED - 5 FCAUSE RECORDS FOUND
```

sui find for dbedit

Purpose

Basic sui find is the simplest case. When using sui find for dbedit, there are additional parameters to include.

Syntax for dbedit

The syntax of sui find when used for dbedit is:

```
sui find source=table
 search=field=value
 noheader delim='";"'
   findtime=1-120_minutes
   maxsave=1-100000_records > file
```

Important!

- Type all the command on one line, without pressing Return within the line. If the line is too long for your window, it will wrap, as illustrated above, but it is really on one line.
- You can abbreviate parts of sui find, as long as you give enough letters to be unique. For example, instead of the example shown above, you can enter.

  ```
  sui find so=table  se=field=value  noh delim='";"' max =1_
  to100000_records > file
  ```

Parameters

This table describes the parameters for sui find when used for dbedit (not for sui find in general).

Parameter	Function

source=*table*
 Example: **sui find source=fcause**
 Output is:
 `Reason Description`
`FIND COMPLETED - 5 FCAUSE RECORDS- FOUND`
`install Installation related`
`routing Network routing error`
`translate Digits translation error`
`testing Network testing related`
`unknown Failure reason unknown`
`FIND COMPLETED - 5 FCAUSE RECORDS FOUND`
	(Required) Selects the database table to retrieve records from.
	 Note:
	 The example has two fields: Reason and Description.

save=*user_filename*	Names the user file in which to store the output of this find. A new file name must begin with an alpha character and contain only alphanumeric or underscore characters. The information is stored as a working set. Default: ws

Parameter	Function

search=*field=value*
Example:
sui find source=fcause search=reason= testing
Output is:
`Reason Description`
`FIND COMPLETED - 1 FCAUSE RECORD FOUND`
`testing Network testing related`
`FIND COMPLETED - 1 FCAUSE RECORD FOUND`
	Recommended. Typically used to get some records from the database table — for example, to delete or modify, or to use as templates for creating new records.
	• *field* is the name of a field in the named database. The
	• *value* is the value to match for the field and can be anything in records. For example, "related" could have been used instead of "testing".
	Search expressions can be much more complex. See "Search expressions" (p. B-29) .

format=*field1,field2:width,field3...*	The fields in the order you want the found records displayed. Enter a list of fields separated by commas (field1,field2:width,field3), a FORM variable, "all", or press RETURN to use the default.
dest= ***destination***	Leave blank to send output to the screen, or enter lp, a printer name, null (for no output), or an ASCII filename.
range	Indicate which records to display.

Parameter	Function

maxsave
=1-100000_records
Example:
sui find source=fcause search=reason=testing noheader delim='";"' maxsave=100000
Output is:
`#Reason;Description`
`testing;Network testing related`
	Recommended. Without this parameter, **sui find** stops at 10,000 records. Some databases (such as those with "route in their names) may be bigger than 10,000. So, use maxsave to move the limit to 100,000 (you cannot go beyond 100,000). In this example, since the retrieval was not cut off, maxsave= has no affect (it does no harm to use it anyway).
	Do NOT use a comma, as in 100,000.
	To see if **sui** find into a file named temp was cut off at 10,000, enter **wc -l temp**
	If output is: "10000 temp", the temp file holds 10,000 lines (10,000 records), so you need a larger maxsave.

fdcgroup=	(optional) Limit output according to an FDC group. To list FDC groups, see "List FDC groups" (p. 7-18) . Default is all.
netgroup=	(optional) If you use the network groups feature; limit output according to a network group or segment. To list network groups, see "List network segments and groups" (p. 7-33) . Default is all.

Parameter	Function
findtime= ***1-120_minutes*** *Example:* **sui find source=cfim findtime=5**	Temporarily overrides the time limit set by the FIND_TIME environmental variable (see "Manage User Environment Variables" (p. 7-47)), which, depending on the table specified, has a initial system default of 10 or 60 minutes. Affects **sui** find on trapalert, alert, cfim. linkalert, mcalert, and otr tables only. In this example, output is limited to CFIMs received in the last 5 minutes. You cannot override the findtime parameter by using **start_datime or end_datime** values. In order to override the findtime parameter, you must do one of the following: • specify a new value for **findtime** search parameter • specify a **date, time** , or **datime** parameter.
netsearch=	(optional) Search using network segment group. Possible values: • all (default) • group (to use netgroup filtering)
fdcsearch=	(optional) Search using fdc group. Possible values: • all (default) • group (to use fdcgroup filtering)

Parameter	Function

delim='";"'
Example:
sui find source=fcause search=reason= testing noheader delim='";"'
Output is:
`#Reason;Description`
`testing;Network testing related`
	(Required) Replaces blanks between fields with semi-colons, to avoid confusion when you later **dbedit** the data. In this example, if you omitted the delim, dbedit would think the record has four fields, "testing", "network", "testing" and "related".
	'";"' is single-quote, double-quote, semi-colon, double-quote, single-quote. If a field must contain a semicolon (;), use another character, such as a colon (:) or enter **Control-a** .

noheader
Example:
sui find source=fcause search=reason= testing noheader
Output is:
`#Reason Description`
`testing Network testing related`
	Recommended. Removes "FIND COMPLETE" lines. Also adds # to the header record, to cause it to be ignored later by the **dbedit** command.

> ***file*** *Example:* **sui find source=fcause search=reason= testing noheader delim='";"' maxsave = 100000 > temp**	Recommended. Directs output into a file. When directed to a file, data does not appear on your screen.

Paging through output

Since the output from sui find may be extensive, it will scroll on your screen, stopping only on the last page. To page through the output, direct it to the operating system pg command: sui find source=fcause | pg

See your operating system manuals for more information on the pg command.

Relationship between MAXSAVE_MAX, MAXSAVE, and noheader

When saving table data with sui find, it is important to understand the relationship between several parameters that can be used to retrieve information:

- MAXSAVE_MAX - a user environment variable, which specifies the maximum value a user can give for the MAXSAVE parameter. The default value is 100,000. The MAXSAVE_MAX upper limit is dependant on table space. Contact Lucent Customer Support before making any change to the range of value for MAXSAVE_MAX
- MAXSAVE - a parameter defined by the user in a sui find command, which specifies the maximum number of user records to save as a result of the sui find. This number can range from 1 to the value set for MAXSAVE_MAX, with a default of 10,000 (unless the MAXSAVE_MAX value is less than 10,000).
- range - a parameter that limits output directed to the screen. The range of values is 1-30,000 with a default of 10,000. This number should be below the MAXSAVE value and within a range of 30,000.
- noheader (noh) - an option which removes "FIND COMPLETE" lines, and adds # to the header record, to cause it to be ignored later by the dbedit command.

To see a listing of your system's current settings for these parameters, enter admset -l (see“admset command” (p. 7-49)).

By default, output to the screen is limited to 10,000 records. You may choose to lower the number of records displayed on the screen by setting MAXSAVE to a lower value. MAXSAVE tells the search to stop at *x* number of records instead of displaying 10,000. MAXSAVE governs both what is saved in the working set (ws) file (also known as User Table) AND what comes to the screen. Increasing MAXSAVE above the screen limit directs the system to save the increased number of records to your working set, but the screen limit remains 10,000.

> **Important!** You cannot specify a MAXSAVE value above that which is set for the system with MAXSAVE_MAX. MAXSAVE_MAX defines the maximum possible value that a user can specify for MAXSAVE.

The noheader (noh) option formats the output to comment out the results lines and the heading, and also removes the screen limitation for saving purposes. This option allows you to save records up to the MAXSAVE_MAX system limitation (default of 100,000 records). If it is set differently, it will save up to the set value if you don't specify a MAXSAVE value in your sui find. This is a useful option when you want to extract data from the Oracle database and redirect the data to a file for use in other software packages, (e.g., reports).

The following examples show different variations of the above mentioned variables used with the sui find command. Each command example is shown with the | *wc* (word count) option, which is useful in showing the size of the output saved to be shown on the screen.

Example: Find using maxsave.

```
sui find so=mean_de |wc

10003 80022 920183

sui list

File                          Type    Size  Last modified


ws                            mean_de 10000 04/06/07 18:17
```

Result: 10,000 records are sent to the screen (the 10003 number above, which includes the 10,000 default records plus 3 header lines) and 10,000 records saved in the working set (ws) file. This is depicted in the Size column of sui list output.

Example: Find using maxsave=20000.

```
sui find so=mean_de maxsave=20000 |wc

10003 80022 920183

sui list

File                              Type    Size  Last modified


ws                                mean_de 20000 04/06/07 18:35
```

Result: A working set file is created with 20,000 records but screen display remains at the default of 10,000 records.

Example: Find using maxsave and noheader.

```
sui find so=mean_de maxsave=20000 noh|wc

20001 80008 920093
sui list

File                            Type    Size  Last modified


ws                              mean_de 20000 04/06/07 18:35
```

Result: A working set file is created with 20.000 records. The noheader (noh) option overrides the screen default of 10,000 and displays 20,000 records.

Example: Find without maxsave variable using noheader option.

```
sui find so=mean_de noh|wc

189070 1512560 17394441
sui list

File                            Type    Size  Last modified


ws                              mean_de 10000 04/06/07 18:13
```

Result: 189,070 records are saved to the screen, no records are saved to the working set (noheader by itself prevents working set creation. Without MAXSAVE or noheader, a working set is created by default).

Search Expressions in sui find

Purpose

In "Syntax for dbedit" (p. B-20) , the sui find syntax to create files for dbedit is described as follows:

```
sui find source=table
 search=field=value
 noheader delim='";"' maxsave=100000 > file
```

The part of the syntax that contains the search expression is: search=field=value

It means retrieve only those records where a specified field equals a specified value. In most cases, this type of search expression is enough. (Sometimes you may even omit a search expression, to retrieve all records.) However, you can also do much more focused searches, as explained in "Search expressions" (p. B-29) .

Search expressions

This table shows different ways to form search expressions. As explained in "Fields" (p. 3-7) , a field can be any of four types. If an expression is limited to certain types, it is noted in the function column of this table. To see a field's type, use field help (see "Table and Field Helps" (p. 3-9) or see the field descriptions in Appendix A, "Reference Database Tables" . In the examples, search expressions are underlined.

Important! Date-time. The following table does NOT give details about search on date and time type fields. Those fields are in surveillance tables, which you do NOT dbedit, and which are explained in Date and Time Fields in Appendix A of the *BB-GUI User's Guide* .

Expression	Function

None
Example:
sui find source=fcause noheader delim='';"' maxsave=100000 > temp
Output in the temp file is:
`#Reason;Description`
`install;Installation related`
`routing;Network routing error`
`translate;Digits translation-`
`error`
`testing;Network testing re-`
`lated`
`unknown;Failure reason unknown`
	If you omit the search expression, **sui find** retrieves all records from the source database.

= search=*field*=*value*
Example:
sui find source=fcause search= reason=testing noheader delim='';"' maxsave=100000 > temp
Output in the temp file is:
`#Reason;Description`
`testing;Network testing related`
	= means "equals". It means retrieve only records that have the value in the field.

Expression	Function

!=
search=*field*!=*value*
Example:
sui find source=fcause search= reason!=testing noheader delim='"; "' maxsave=100000 > temp
Output in the temp file is:
`#Reason;Description`
`install;Installation related`
`routing;Network routing error`
`translate;Digits translation-error`
`unknown;Failure reason unknown`
	!= means "not equals". It means retrieve records that do NOT have the specified value in the field
	You cannot use != with date-time type fields.

-, ?, or ~ **search=*field*=-** *Example:* **sui find source=fcause search=description="-" noheader delim='";"' maxsave=100000 > temp** Output in the temp file is: `#Reason;Description`	These are null characters meaning retrieve records where a field is blank. Most often, you use "-". (For when to use three null characters, see "Null characters" (p. 3-8) .) **Note:** You cannot use null with date-time type fields. If there is one key field, it cannot be null. That is why this example uses the non-key description field. If the search string contains a '-', it is treated as a range specification. If a '-' needs to be included in the search string, the string should be enclosed in a pair of single and double quotes. For example, entering: **sui find so=rearch se=conv=dms-mtx** will produce an error However, entering: **sui find so=rearch se=conv='"dms-mtx"'** will display rearch entries for conv type of 'dms-mtx'.

Expression	Function

Multiples in one field
search=*field1, field2, field3*
Example:
sui find source=fcause search= reason=testing,routing
noheader delim='";"' maxsave= 100000 > temp
Output in the temp file is:
`#Reason;Description`
`routing;Network routing error`
`testing;Network testing related`
	Match one field to any of several values. The example means, retrieve records where "reason" is either "routing" or "testing".
	You MUST use commas (not spaces).

and **search=*field1=value1 and field2= value2*** *Example:* **sui find source=fcause search= reason=testing and description="-" noheader** delim="";"" maxsave=100000 > temp In this example, no records met both conditions, so there is no output in the temp file.	If you use "and" among two (or more) fields, BOTH (or more) matches must be met. The example means, retrieve records where "reason" is "testing" and "description" is "-". (In the example, no records met both conditions.) You can also use "and not". To use the words "and", "or", or "not" as a value *within* a search expression, enclose the word in both single and double quotes. *Example:* **sui find so=nbi_config se=nbi_id= ' "and" '**

or
search=field1=value1 or field2= value2
Example:
sui find source=fcause search=reason=testing or description="-" noheader delim="";"" maxsave=100000 > temp
Output in the temp file is:
`#Reason;Description`
`testing;Network testing related`
	If you use "or" among two (or more) fields, ANY matches apply. The example means, retrieve records where "reason" is "testing", or "description" is "-".
	You can also use "or not".
	To use the words "and", "or", or "not" as a value *within* a search expression, enclose the word in both single and double quotes.
	Example:
	sui find so=nbi_config se=nbi_id= ' "or" '

Expression	Function

*
search=*field=string_with_
_*
Example:
sui find source =fcause search=reason="t*" noheader delim=";" maxsave=100000 > temp
Output in the temp file is:
`#Reason;Description`
`translate;Digits translation error`
	Asterisk (*) is a wild card meaning any number of letters. It can be used before (*abc) in (a*bc) and after (abc*).The example means retrieve records where "reason" is any value starting with letter t.
	A less used wild card is ampersand (&), meaning any one letter.
	You cannot use wild cards with numeric or date-time type fields.

Range **search=*field=number-number*** *Example:* **sui find source=swarch search= hnpa=100-1503noheader** delim=";" maxsave=100000 > temp	This is a range of numbers. The field must be numeric or date-time. That is why this example uses the swarch source table, whose hnpa field is numeric.

>, <, >=,**search=*field /< a_number***
Example:
$ sui find source=rearch search= tag/>1 noheader delim='";"' maxsave=100000
Output in the temp file is:
`#Re;Source;Tag;Conv;Down;De-graded;Interval;Calc;Sam-pling;Tz;Release`
`admstx0101t;kscp1;58;4ess;0;0;100;y;-;-;-`
`akrnoh2505t;kscp1;43;4ess;0;0;100;y;-;-;-`
`albqnmma02t;kscp1;54;4ess;0;0;100;y;-;-;-`
`anhmca0211t;kscp1;70;4ess;0;0;100;y;-;-;-`
`argvbcaa41t;kscp1;46;4ess;0;0;100;y;-;-;-`
`austtxgr07t;kscp1;12;4ess;0;0;100;y;-;-;-`
`bltnin0144t;kscp1;44;4ess;0;0;100;y;-;-;-`
`chcgilcg51t;kscp1;76;4ess;0;0;100;y;-;-;-`
`chcgilcl11t;kscp1;29;4ess;0;0;100;y;-;-;-`
`chcgilcl59t;kscp1;20;4ess;0;0;100;y;-;-;-`
	This is greater than, less than, less than or equal to, or greater than or equal to.
	The field must be numeric or date-time. That is why this example uses the swarch source table, whose hnpa field is numeric.
	You must type a backslash(/), in front of >, <, >=, or <= contained in the search expression (but not in front of symbol to redirect the output to the temp file).

sui help Command

Purpose

The sui help command explains FDCs.

Syntax

```
sui help item=fdc=fdc1,fdc2...fdc10
```

Parameter	Description
(required) **item=**	Up to ten FDCs separated by commas, no spaces

Example

```
sui help item=fdc=nca,vca
```

Since the output from sui help is extensive, it will scroll on your screen, stopping only on the last page. To page through the output, direct it to the operating system pg command: sui help item=fdc-nca,vca | pg

See your operating system manuals for more information on the pg command.

sui join Command

Purpose

The sui join command combines two user files (databases) into one user file.

Reference: Other commands for user files (databases) are: "sui list Command" (p. B-40), "sui remove Command" (p. B-42), "sui rename Command" (p. B-44), and "sui sort Command" (p. B-51).

Syntax

```
sui join from=user_file to=user_file
```

Parameter	Description
from (required)	The source file you are copying into the destination file. This file is not changed. The source and destination files must: • Have different names. • Hold the same type of records (such as CFIMs) Nonrestricted users can indicate another user's file by including the user ID followed by a slash prior to the file name. Example: *sjm/rpt94*
to (required)	The source file is added to the end of the destination file.

Example

```
sui join from=cfims_812 to=cfims_811
```

sui linkmon Command

Purpose

The **sui linkmon** command is for daily monitoring of the links between reporting entities (listed in rearch table) and sources (see “Sources” (p. 1-17)). Sources collect CIMs from the reporting entities in the network and forward them to the NTP host. The **sui linkmon** command enables you to check how reliably the communications links between switches and sources and between the sources and NTP are supplying NTP with data.

Important! The sui linkmon command is one of the methods to monitor links when administering CIM sources. See Chapter 13 "CIM Source Administration", section “Monitor Links” (p. 5-51) for more information.

Description

The **sui linkmon** command displays link alert records listing the status of data links between NTP and sources and between sources and the reporting entities in their respective domains. NTP determines that a link is degraded or down based on messages (or lack of them) from the source, and generates a link alert record when a link becomes degraded or fails. The NTP database that triggers the status level of the "link" is based on three fields in the rearch table: down, degraded, and calc. A link may be listed as down or degraded because:

- The switch-source link is down or degraded
- The source-NTP link is down
- The CIM count for the specified interval (in rearch database table record for the type of switch that is reporting) is below either the degraded or down threshold for the type of switch that is reporting.

Syntax

sui linkmon

sui linkmon runs continuously, refreshing the screen every minute (unless there are no new messages), until you press the **Delete** key to terminate.

Important! To see a static display and to get additional information from the NTP linkstatus database by entering **sui find source=linkstatus se=status=up**

Output

This example shows output from the **sui linkmon** command.

```
Datime Re Source Status Type Reason Cims
01/02/21 13:21 sva12 - degraded sccs reframed 253
01/02/23 15:03 sva16 - degraded sccs reframed 10
```

sui linkmon output fields

This table lists sui linkmon output fields.

Field	Purpose
Datime (date and time)	Combines the data in the date and time fields in the format YY/MM/DD hh:mm. This field exists in the linkalert table record, but is not displayed unless specified in your LINKALERT_FORM variable. • *Date* — The date on which the link alert was generated and stamped by the NTP system clock. It is an 8-character field in the format yy/mm/dd • *Time* — The time at which the link alert was generated and stamped by the NTP system clock. It is a 5-character field in the format hh:mm, where hh can be 0-23 and mm can be 00-59
RE (reporting entity)	ID of the RE or source reported on.
Source	Names the source that collects CIMs from the RE. It shows "-" for "Not Applicable" when the source itself is the RE.
Status	Gives the status (down, degraded, or unknown) of the link reported on.
Type	The types of sources for the link alert status. Values for this field are: • *sw* (switch) — If the RE-to-source link is down or degraded • *cp* (communications processor) - If the CP-to-NTP link is down, and the RE-to-CP status is unknown. • *ems* — If the EMS source-to-NTP link is down, and the RE-to-ISA status is unknown. • *cim* — If the status is determined based on low CIM counts • *sccs* — switch control central system • *re* — reporting entity • *univ* — universal interface • *osps* — operator service position system • *tops* — traffic operator position system • *tms* — tnm surveillance module
Reason	The reason (code) for the link status. See "sui linkmon reason codes" (p. B-38) .

Field	Purpose
Cims	Number of CIMs in the current interval (as defined in the rearch table for the entity type of this RE). If the RE is not a source, this is the number of total messages received in the last 5-minute interval.

Sui linkmon troubleshooting

Look on **`sui linkmon`** output at all rows for the source you are troubleshooting. You are interested in any rows that show tallies of 0 (zero).

Rows with tallies of 0...	Guidelines
NO rows	The links are most likely healthy
SOME rows	You must find out why some switches are not sending CIMs to the source. Be sure you administered the rearch table for each switch from which the source collects data.
ALL rows	Either: • Switches are not sending CIMs to the source. Be sure you administered the rearch table for each switch from which the source collects data. • Switches are sending CIMs to the source, but the source is not forwarding them to NTP.

sui linkmon reason codes

This table lists codes you may see in the Reason field of `sui linkmon` output.

Code	Meaning
carrier	The carrier from the entity to the ISA is dropped.
closed	The NTP port to the source is closed.
degraded	The number of CIMs received for a given RE is equal to or has fallen below the threshold specified in the “rearch Table” (p. A-129) .
down	The source is down or, in the case of an RE, the value for the source is equal to or has fallen below the threshold specified in the “rearch Table” (p. A-129) .
lf1	The link failure down threshold has been exceeded.
lf2	The link failure degraded threshold has been exceeded.
logging	The ISA reports that it is not logging a particular entity.

Code	Meaning
no io proc	The I/O process isn't running or hasn't received an update.
no lsm	No link status message received from the CP.
no record	No record for a specific entity, either because no entity record existed in the link status message or no link status message was received.
reframed	Framing is out of sequence in the source to NTP link.
rhst	The link to the remote host is down.
status bit	The link status message reports the switch to CP link is down.
startup	Due to recent startup (or interval increase), the messages received are below the down or degraded thresholds.
timed out	Have not received a message from the source in the interval specified.
um1	The unreadable messages "down" threshold has been exceeded.
um2	The unreadable messages "degraded" threshold has been exceeded.
zm	The zero messages interval has been exceeded.

sui list Command

Purpose

The **sui list** command lists user files (databases) created from any NTP interface, for your current login ONLY. This is a NTP command. It is not found in *Oracle* references.

To use **sui list** , you can be in any directory, but you must log on as the user whose databases files you want to list.

> **Important!** The sui list command is most often used when modifying users. See Chapter 7, "Modify Users" for more information.

Reference: Besides **sui list** , commands for user files (databases) are: "sui join Command" (p. B-35)), "sui remove Command" (p. B-42) , "sui rename Command" (p. B-44) , and "sui sort Command" (p. B-51) ,

Alternate command

You can also use the **ptspace** command (see "ptspace Command" (p. 7-59)) with a login ID in its username parameter. **Ptspace** is simpler to use.

Syntax

```
sui list [files=userfile1, userfile2...]
```

With no parameters, **sui list** shows all database files created from any NTP interface for the current login ID.

Parameter	Description
files (optional)	Restricts the list of user database files to be displayed. Separate multiple expressions with commas. You can use the * metacharacter in database names (see "Search Expressions in sui find" (p. B-29)).

Example

To list all user database files named beginning with "cfim" for your current login enter

```
sui list files=cfim*
```

Output

Output is a list of databases files created by the user you are logged in as. Output has the following parts:

Field	Function
File	Name of the database file, which was named when the user did a **find** . Please note that databases whose names include "ws" were named automatically and are automatically overwritten. Other databases were named by users, and persist until manually removed.
Type	The name of the system database where the user was doing a **find** when the user-created database file was created.
Size	The size of the user database file bytes.
Last modified	When the use database file was created or overwritten.

Output example

You log on as a user you want to check, and, in any directory, enter **sui list** . Output is:

```
File              Type        Size          Last modified
dave1             notify      1             00/01/01 02:37
ws                outdkdial   22            99/12/31 23:25
ws_view           cfim        10000         00/01/01 02:35
ws_view_prev      cfim        1048          00/01/01 02:34
```

sui remove Command

Purpose

The **sui remove** command removes user files (databases) created from NTP interfaces. This is a NTP command. It is not found in *Oracle* references. You must be logged on as **ntp** to use **sui remove**. It does not matter which directory you are in — results are the same.

This command is useful if a user has accumulated too many user databases file and is not available to remove them (see "How users create and remove databases (user files)" (p. 7-54) for how users remove their own database files).

> **Important!** Typically you remove only user databases files, which are in the user table space. Removing databases from other table spaces may be dangerous.

Reference: Other commands for user files are "sui join Command" (p. B-35), "sui list Command" (p. B-40), "sui rename Command" (p. B-44), and "sui sort Command" (p. B-51).

Syntax

```
sui remove [force] files=login/userfile1,login/userfile2
```

Parameter	Description
force (optional)	• Omit if removing databases files that belong to your current login. • Use if removing another user's files (system administrators only).
files=*login/userfile1*,*login/userfile2* (required)	Lists one or more user database files to be deleted (use commas to separate filenames). You can use the * metacharacter in database names (see "Search Expressions in sui find" (p. B-29)). • *login* — (optional) Login ID whose database you are deleting. Use only if deleting for a login other than your current login. • *database* — (required) Name of database you are deleting.

Examples

- To delete a database files named daves belonging to your current login, enter
  sui remove files=daves
- To delete database file mary1 belonging to login mtm (not your current login), enter
  sui remove force files=mtm/mary1
- To delete database files mary1 and mary2, belonging to login mtm, (not your current login) enter
  sui remove force files=mtm/mary1,mtm/mary2

Important! The mtm/mary1 and mtm/mary2 in the examples above are NOT paths. They are login_ID/database_ name.

Output

This command has no output.

sui rename Command

Purpose

The sui rename command changes the name of a user file (database).

Important! If you rename to a file name that already exists, the file is overwritten.

Reference: Other commands for user files (databases) are: "sui join Command" (p. B-35), "sui list Command" (p. B-40), "sui remove Command" (p. B-42), and "sui sort Command" (p. B-51).

Syntax

```
sui rename from=userfile1 to=userfile2
```

Parameter	Description
from (required)	Requires the name of the user file you want to rename. This file must already exist.
to (required)	Requires the new or existing user file name to which you are renaming the data.

Example

To rename a user file called trapout to traprpt, enter

```
rename from=trapout to=traprpt
```

sui set Command

Purpose

This command defines the following for YOUR login:

- Environment variables. These determine such things as your FDC group and what fields you see when you run Ascreen from the SUI.
- User variables. These are expandable strings, used, for example to represent a long list of CLLIs you do not want to type repeatedly. Precede it with the $ character and enclose it in single quotes. Example: sui '$myfindf1'

Reference:

- To set environment variables for another user, or for the system default, use admset (see "Reprocess CDRs" (p. 10-42)). You do NOT set user variables for another user, or system-wide.
- sui set is NOT related to sui setsys for thresholding variables.

Syntax

```
sui set [variable=variable_name value='"value" ]
```

Parameter	Description
variable (optional)	The environment or user variable you will set. Reference: For the list of environment variables, see "User environment variable list (admset)" (p. 7-50).
value (optional)	The value you are assigning. Omit to unset (remove) a variable. Nest the value in double, and then single quotation marks. For example: **sui set variable=RANGE value='"30001 - 50000"'**

List variables

Overview

To list environment and user variables specific to YOUR login only, enter **`sui set`**.

Important! To list ALL variables recognized for your login, use the operating system enter set (or to page the list, enter **`set | pg`**)

Set a variable

Overview

Use the value= parameter to set variables:

- Environment variable. To set your login's TERMINAL variable to vt100, enter (in this case, you can omit the double and single quotation marks around vt100, but it would hurt nothing to include them):

  sui set variable=TERMINAL value=vt100

- User variable. To unset a user variable named mytrap, enter (note the double and single quotation marks):

  sui set variable=mytrap value='"trapcfim se=fdc=900 and re=arlnht0504t and digits=8007931212"

  'To use the mytrap variable for shorthand entry in the command line, enter sui '$mytrap'

Unset variables

Procedure

To unset a variable, omit the value= parameter:

Examples

- Environment variable. To unset your login's TERMINAL variable back to system default, enter

  sui set variable=TERMINAL

- User variable. To unset (remove) a user variable named mytest, enter

  sui set variable=mytest

Use a user variable in the SUI

Overview

To use the variable in the SUI, enter the variable name preceded by a $ character surrounded by single quotes

```
sui '$myfindf1'
sui find se='$mysearch'
```

sui setsys Command

Purpose

This command is used to view or modify values of the NTP system variables that define link alerts or thresholding variables. System variables are initially set to default values during installation.

Important! **`sui setsys`** is NOT related to **`sui set`** for either environment or user variables.

Example:

- For example of setting a **`MCTHRESH`** variable see "MCTHRESH variable" (p. 8-52)

Syntax

```
sui setsys [variable=variable_name value='"value"']
```

Parameter	Description
`variable`	The system variable you will set. Reference: For the list of all variables on your system, enter **`sui setsys`**.
`value` (optional)	The value you are assigning. Omit to set a default value.

sui sort Command

Purpose

The sui sort command reorders records in a user file (database), by the column or columns you choose, in ascending or descending order.

Reference: Other commands for user files (databases) are: "sui join Command" (p. B-35), "sui list Command" (p. B-40), "sui remove Command" (p. B-42), and "sui rename Command" (p. B-44).

Syntax

```
sort file=userfile save=user_filename field=field1:a/d,field2:a/d,
   ...format=format
```

Parameter	Description
file (optional)	Default: ws. Names the user file containing the data to be sorted. Metacharacters are not allowed in this parameter. Nonrestricted users can indicate another user's file by including the user ID followed by a slash prior to the file name, for example: *sjm/rpt94*
save (optional)	Names the user file in which to store the newly sorted records. A new file name must begin with an alpha character and contain only alphanumeric or underscore characters. Default: ws
field (optional)	Names the field(s) on which the records are to be sorted. When multiple fields are entered in this value, records are sorted based on the order of those fields. Enter each field using the format: **field:order** *Example:* **fdc:a,lcnt:d**
format (optional)	Selects output screen format. Options are: • Enter **all** to display all the fields. • Enter a list of field names separated by commas in the order you want. **format=fdate,ftime,ldate:5,ltime, ne,type,fdc,tc,tn, cnt5,cai5,cnth,caih,owner** • To change field size, follow the field name with colon and number of characters. **format=fdate:5,ltime:5, ne:16**

Example

To sort records in the working set (ws) database by the records' count field in descending order, enter sui sort file=ws field=count:d

sui trapalert Command

Purpose

The sui trapalert command shows each new alert case, within the 5-minute period when it is created, but before the end of the period, when the alert case moves to Ascreen. (For how to read Trapalert, see the *BB-GUI User's Guide*.)

Important! Trapalert automatically updates. Exit by pressing the Delete key.

Syntax

```
trapalert search= [not] field=value1... and/or [not]
field=value1,value2... format=field1,field2:width,field3...
fdcgroup=all/group_name netgroup=all/group_ name
```

These parameters apply one time when entered. To permanently change a parameter for your login, use the admset command on your environment variables (see "Reprocess CDRs" (p. 10-42)).

Parameter	Description
search (optional)	Selects which alert cases appear on Trapalert. Omit to see all. Reference: For how to build search expressions, see the *BB-GUI User's Guide*.
format (optional)	Selects output screen format. Options are: • Enter **all** to display all the fields. • Enter a list of field names separated by commas in the order you want. **format=fdate,ftime,ldate:5,ltime,ne,type,fdc,tc,tn, cnt5,cai5,cnth,caih,owner** • To change field size, follow the field name with colon and number of characters. **format=fdate:5,ltime:5, ne:16**
fdcgroup=all or a group_name (optional)	Limit output according to an FDC group. To list FDC groups, see "List FDC groups" (p. 7-18).
netgroup=all or a group name (optional)	If you use the network groups feature; limit output according to a network group or segment. To list network groups, see "List network segments and groups" (p. 7-33).

Example

To call up Trapalert output, enter **sui trapalert**

sui trapcfim Command

Purpose

The sui trapcfim commands shows each new cfim as it arrives.

Important! Trapcfim automatically updates. Exit by pressing the Delete key.

Syntax

```
sui trapcfim search= [not] field=value1... and/or [not]
field=value1,value2...
format=field1,field2,... numr=numrows
```

Important! These parameters apply one time when entered. To permanently change a parameter for your login, use the admset command on your environment variables (see "Reprocess CDRs" (p. 10-42).

Parameter	Description
search (optional)	Selects which alert cases appear on Trapalert. Omit to see all. Reference: For how to build search expressions, see the *BB-GUI User's Guide*.
numrows (optional)	Sets the number of rows in the display window (for layers on an AT&T 630 or 730 terminal). Valid values are whole numbers between 10 and 60. If no value is entered, the TRAPCFIM_ROWS environment variable sets the number of rows.
format (optional)	Selects output screen format. Values: • **all** — displays all the fields. • Enter a list of field names separated by commas in the order you want. **format=fdate,ftime,ldate:5,ltime, ne,type,fdc,tc,tn, cnt5,cai5,cnth,caih,owner** • To change field size, follow the field name with colon and number of characters. **format=fdate:5,ltime:5, ne:16**

Example

To run Trapcfim to show each new CFIM with FDC 63, enter

```
sui trapcfim search=fdc=63
```

sui trapdata Command

Purpose

The sui trapdata commands shows each new cfim in selected data source as it arrives.

Important! Trapdata automatically updates. Exit by pressing the Delete key.

Syntax

```
sui trapdata source=table
search= [not] field=value1... and/or [not]
field=value1,value2...
format=field1,field2,... numr=numrows
```

Important! These parameters apply one time when entered. To permanently change a parameter for your login, use the admset command on your environment variables (see "Reprocess CDRs" (p. 10-42).

Parameter	Description
source	Selects which data source is observed.
search (optional)	Selects which alert cases appear on trapdata. Omit to see all. Reference: For how to build search expressions, see the *BB-GUI User's Guide*.
numrows (optional)	Sets the number of rows in the display window (for layers on an AT&T 630 or 730 terminal). Valid values are whole numbers between 10 and 60. If no value is entered, the TRAPCFIM_ROWS environment variable sets the number of rows.
format (optional)	Selects output screen format. Values: • **all** — displays all the fields. • Enter a list of field names separated by commas in the order you want. **format=fdate,ftime,ldate:5,ltime, ne,type,fdc,tc,tn, cnt5,cai5,cnth,caih,owner** • To change field size, follow the field name with colon and number of characters. **format=fdate:5,ltime:5, ne:16**

Example

To run Trapdata to show each new CFIM with FDC 63, enter

```
sui trapdata source=cfim search=fdc=63
```

Appendix C: Application Backup and Recovery

Overview

Purpose

This appendix tells how to back up and recover the Network Trouble Patterning software application and databases, and provides information for designing a backup strategy.

Contents

Introduction

Introduction To Backup Strategy

Responsibility for backup strategy

The NTP administrator is responsible for backing up and recovering the NTP application and databases. We cannot detail a backup strategy for every type of installation or customer scenario. However, NTP provides several utilities that are documented here to assist you in developing a backup strategy.

Scope

Backups made with these utilities are designed to be used in conjunction with standard vendor utilities for your operating system and platform. NTP backups are NOT alone suitable for recovery of entire disks or non-NTP disks.

Reference

- See the documentation for the standard backup and recovery utilities for your operating system and platform to perform such tasks as creating a bootable tape for use in disaster recovery scenarios, establishing disk mirrors, and recovering files or disks from a mirror.
- See “Application Directory Structure” (p. 1-33) for a full description of the NTP file system and directory structure.

Cautions

Catastrophic data loss that requires reinstallation to recover is possible even on systems that use fault tolerant hardware if an error corrupts or deletes all mirrored or backup copies of any Oracle data file. Examples of such errors are corruption of operating system, Oracle, or NTP data; administrator error (removing files); or malicious intruder activity. For this reason, a sound backup and recovery strategy is necessary.

NEVER use a mechanism (such as third-party backup software) that backs up NTP's Oracle databases directly, without any special preparation by the NTPapplication. Copies of Oracle data files made from a running NTP system always corrupt the database if they are restored. The utilities described in this appendix prevent this by making backups from either an idle (cold, non-volatile) mirror of the NTP file system or exported copies of the data.

If an NTP installation is corrupted due to hardware failure, such as loss of a disk, the initial task is always to recreate the NTP file system. The procedure for this varies by hardware configuration and operating system. Consult the vendor documentation for your system, or a vendor service representative for assistance. Contact your NTP support

organization, if necessary. Once a file system — empty and of sufficient size — is created, the NTP application can be restored.

Commands for Application Backup and Recovery

Introduction

Purpose

NTP provides a core set of commands for use in standard backup and recovery scenarios. Other utilities are also provided for use in custom strategies. Customers participating in an enterprise management backup system, for example, may have use for these utilities. The following two tables summarize the core and custom utilities.

Consult your NTP support organization to ensure that your backup strategy and the utilities you use are appropriate.

Commands for standard backup and recovery scenarios

This table briefly describes the available utilities for use in custom backup and recovery. For more detail, see the individual descriptions in the references.

Command	Summary	Reference	Use
exp_db	Converts the *Oracle* reference data and user working sets (user files) to ASCII files using the *Oracle* export utility, and stores the files in $ORAEXPORT for recovery with **imp_db**.	"exp_db Command" (p. C-8)	Backup to $ORAEXPORT
imp_db (and imp_ws)	Converts system tables backed up by **exp_db** as files in $ORAEXPORT back to databases. The **imp_ws** command does the same for working sets (user files, "ws" files) exclusively.	"imp_db (and imp_ws) Command" (p. C-10)	Recovery from $ORAEXPORT
restore_ldap	Restores LDAP Database from file.	"restore_ldap Command" (p. C-13)	After executing **save_ldap**
save_ldap	Saves LDAP Database to `ldap.tar` file in the speciefied directory.	"save_ldap Command" (p. C-12)	

Commands for custom backup and recovery scenario

NTP provides the following commands for custom backup and recovery scenarios.

Command	Summary	Reference
db2ascii	Saves NTP databases (including reference data, working sets) and the *Oracle* control file in ASCII representation.	"db2ascii Command" (p. C-7)
ntp_dbfiles	Outputs a list of files that can NOT not be backed up while the *Oracle* database is open without damaging the *Oracle* database if a restore is done.	"ntp_dbfiles Command" (p. C-11)

db2ascii Command

Purpose

The NTP **db2ascii** command saves various NTP databases in ASCII representation.

This command uses the **exp_db** (see "exp_db Command" (p. C-8)) command to create ASCII representations of the NTP reference data, the user working sets (user files), and the Oracle control file.

In certain circumstances you can use the saved data to recover portions of NTP data.

Permission

Only the **ntp** login can run **db2ascii**. If you are not logged in as **ntp**, the command prompts you for the **ntp** password.

Syntax

db2ascii

There are no arguments or options for **db2ascii**.

Output

This command does not of itself return a response to the screen. However, it returns an exit code of 0 if successful. If any of the constituent commands fails, you get the response from the respective command, and the exit code for **db2ascii** is 1.

- Output from **exp_db** goes to $ORAEXPORT/LOG, $ORAEXPORT/DMP, and $ORAEXPORT/PARAM

exp_db Command

When to use

Useful to provide backups of databases without requiring tape.

Purpose

The NTP **exp_db** command converts the Oracle reference data and user working sets (user files) to ASCII files using the Oracle export utility, and stores the files in $ORAEXPORT. If you need to recover databases, you can do so from these files, without loading backup tapes.

This table illustrates which databases **exp_db** converts. You can NOT select which tables are converted.

For these system tables...	exp_db backs up...
Reference. Contain data from system administrators (*see Appendix A, "Reference Database Tables")	All files in Oracle REFERENCE table space.
Working sets (user files). Contain data saved as working sets or user files These are "ws" databases NTP creates automatically in user "find" operations, and databases that users can save manually from working sets or through the **sui find** command.	All files in Oracle USR table space
Surveillance data. Contain data from Re's (see Appendix A of the *BB-GUI User's Guide*).	ONLY acase (active alert case).

Note

- The system does NOT stop during conversion.
- Mirrors are not split. The system runs in "safe" mode
- The converted files are in $ORAEXPORT/DMP. Each file has a .dmp suffix.

Permission

Only the **ntp** login can run **exp_db**.

Syntax

exp_db

This command has no parameters. Enter only **exp_db**

Output

Output from `exp_db` goes to:

- $ORAEXPORT/LOG
- $ORAEXPORT/DMP
- $ORAEXPORT/PARAM

As the command executes, it outputs messages to the screen, ending with the following message indicating successful execution:

```
Export terminated successfully without warnings.
```

exp_db from cron

The **exp_db** command runs automatically, daily from **cron**. You can also run it manually, if needed.

It also runs as part of **applbackup** with no options, **file_backup**, and **db2ascii**.

Reference

- To back up tables with **exp_db**, see "Back Up Application Databases to $ORAEXPORT" (p. C-14).
- Recovery
  - To recover system tables from $ORAEXPORT, see "Recover System Tables from $ORAEXPORT" (p. C-17).
  - To recover working sets from $ORAEXPORT, see "Recover Working Sets from $ORAEXPORT" (p. C-24).
  - **exp_db** does NOT convert surveillance data (except acase), because they change rapidly.

imp_db (and imp_ws) Command

Purpose

The NTP **imp_db** command recovers system tables by converting system tables (backed up by **exp_db** as files in $ORAEXPORT) back to databases. This enables you to recover system tables without loading backup tapes. The **imp_ws** command does the same for working sets (user files, "ws" files) exclusively. Both commands are in $APPLBIN.

Reference

- *Procedures.* For use of **imp_db**, see "Recover System Tables from $ORAEXPORT" (p. C-17). For use of **imp_ws**, see "Recover Working Sets from $ORAEXPORT" (p. C-24).
- *Which system tables.* For which system tables are in $ORAEXPORT, see "exp_db Command" (p. C-8).
- *Backup.* For how to back up system tables (and working sets) to files in $ORAEXPORT, see "Back Up Application Databases to $ORAEXPORT" (p. C-14).

Note

- *Downtime.* Before using this command, you must stop NTP. Procedures in this chapter tell you how to do this (using **ntpstop**).
- *How Current?* To see how current the files are that you are converting back to databases, you can list the contents of $ORAEXPORT/DMP. (Since **exp_db** runs daily from **cron**, files are at least as current as yesterday's date.)

Permission

Only the **ntp** login can run **imp_db** (and **imp_ws**).

Syntax

$APPLBIN/imp_db

or

$APPLBIN/imp_ws

This command has no parameters. Enter **imp_db** or **imp_ws** and then follow the prompts.

The **imp_db** command prompts you to import selected files, all BUT selected files, or all files. For details, see "Recovery strategy for system tables" (p. C-17).

ntp_dbfiles Command

Purpose

The **ntp_dbfiles** command provides a list of files that comprise the NTP Oracle database, including Oracle control and data files.

- These files should NOT be backed up during incremental or other file-based backups unless the Oracle database is closed.
- These files MUST be backed AS A SET up for a complete cold database backup.

  Important! It the files listed by **ntp_dbfiles** are backed up and then restored while the Oracle RDBMS is running, the Oracle database will be damaged.

Permission

Any user with a valid *Oracle* environment can run **ntp_dbfiles**.

Syntax

ntp_dbfiles

There are no arguments or options for **ntp_dbfiles**.

Output

This command returns a list of files and directories to stdout.

save_ldap Command

Purpose

The **save_ldap** command saves the LDAP Database to the *ldap.tar* file, in the specified directory.

Important! save_ldap interacts with the Scheduled Data Distribution (SDD) feature which uses LDAP Database to retrieve E-mail addresses. The command stops the OpenLDAP deamon for a few seconds while the data is restored. While the LDAP deamon is down, you will not be able to log into the BB-GUI and SDD jobs will not be able to retrieve email addresses. BB-GUI users who are already logged in will not be affected.

Reference: For detailed information on the Scheduled Data Distribution feature, see *BB-GUI User's Guide, chapter 5, Analyze*.

Permissions

Only the **ntp** login can run **save_ldap.**

Syntax

save_ldap [-a] [-d <dest dir>]

Parameter	Purpose
-a	Saves all local LDAP info.
-d <dest dir>	Use *-d <dest dir>* to specify the destination directory. The default directory is **/lucent/ntp/oraexport.**

restore_ldap Command

Purpose

The **restore_ldap** command restores the LDAP Database from the *ldap.tar* file created earlier with the **save_ldap** (see "save_ldap Command" (p. C-12)).

Important! **restore_ldap** interacts with the Scheduled Data Distribution (SDD) feature which uses LDAP Database to retrieve E-mail addresses. The command stops the OpenLDAP deamon for a few seconds while the data is restored. While the LDAP deamon is down, you will not be able to log into the BB-GUI and SDD jobs will not be able to retrieve email addresses. BB-GUI users who are already logged in will not be affected.

Reference: For detailed information on the Scheduled Data Distribution feature, see *BB-GUI User's Guide, chapter 5, Analyze*.

Permissions

Only the **ntp** login can run **restore_ldap**.

Syntax

```
restore_ldap [-s <source dir>]
```

Parameter	Purpose
-s <source dir>	Use *-s <source dir>* when the specified destination directory was different from the default one: **/lucent/ntp/oraexport**.

Application Backup Procedures

Back Up Application Databases to $ORAEXPORT

Purpose

This procedure uses **exp_db** to convert system tables and working sets (user files) in the Oracle databases to files in the $ORAEXPORT/DMP directory, from which you can recover without loading backup tapes.

References

- For which system tables are converted to files, see "exp_db Command" (p. C-8).
- For how to recover system tables and user files from $ORAEXPORT to databases, see "Recover System Tables from $ORAEXPORT" (p. C-17).and "Recover Working Sets from $ORAEXPORT" (p. C-24).

When to use

exp_db runs automatically, daily from **cron**, and whenever you run **db2ascii**. You would rarely run this command manually — typically only before you do something risky, such as major database changes.

Back up databases to files

Procedure

Use this procedure to convert databases to files in $ORAEXPORT.

1 Log on the NTP host as **ntp**. (You must be logged on as **ntp** to proceed.)

2 Enter **$APPLBIN/exp_db**

Result: The command produces many lines of output to the screen, ending with this line indicating successful execution:

```
Export terminated successfully without warnings.
```

For more information on the **exp_db** command, see "exp_db Command" (p. C-8).

END OF STEPS

Application Recovery Procedures

Application Recovery Overview

Guidelines

Data loss often means you have a problem your NTP support organization needs to know about. They can advise you on which recovery strategy is best. ALWAYS contact the NTP support organization in the following cases:

- Before recovering databases (system tables).
- If you plan to restore ALL files from all file systems (Problems may occur when you restore all copies of the Oracle control files during this type of recovery.)
- If disk corruption or failure made a database inoperable (In severe cases, the only way to recover from a database corruption may be to reload NTP and rebuild the entire database.)

If you mis-edited a system table and you want to recover it to correct your mistakes, it is usually safe to do so.

Recovery utilities

Purpose	Command	Reference
Do file-to-database conversion, recovering system tables saved in $ORAEXPORT with **exp_db**.	**imp_db** (and **imp_ws**) **Note:** The **imp_ws**command converts working sets (user files) only.	• "imp_db (and imp_ws) Command" (p. C-10) • "Recover System Tables from $ORAEXPORT" (p. C-17) • "Recover Working Sets from $ORAEXPORT" (p. C-24)

Recover System Tables from $ORAEXPORT

Purpose

The various procedures to recover system tables (see "Recovery strategy for system tables" (p. C-17)) all work in a similar way. They convert the system tables that were backed up as files in $ORAEXPORT back to databases. This enables you to recover databases without loading backup tapes.

References

- For which system tables are converted to files, see "exp_db Command" (p. C-8).
- For how to convert system tables in databases to files in $ORAEXPORT, see "Back Up Application Databases to $ORAEXPORT" (p. C-14).

Before you begin

The system table files that were converted from databases are at $ORAEXPORT/DMP. Each has a .dmp suffix. Check there to be sure the files you want exist. If they do not, recover the files from tape.

Recovery strategy for system tables

There are three ways to use **`imp_db`** to recover tables.

To recover...	Reference...
One or more of the following system tables ONLY: systeminfo, custid, active acase, or vpnid	"Recover systeminfo, custid, acase or vpnid from $ORAEXPORT" (p. C-18)
All system tables EXCEPT systeminfo, custid, active acase, or vpnid	"Recover all BUT systeminfo, custid, acase, or vpnid from $ORAEXPORT" (p. C-20)
All system tables	"Recover all tables from $ORAEXPORT" (p. C-22)

Recover systeminfo, custid, acase or vpnid from $ORAEXPORT

Procedure

This procedure uses the **imp_db** command to one or more of the listed tables (and NO other tables) from $ORAEXPORT. The procedure requires you to use the **ntpstop** and **ntpstart** commands to stop and restart NTP For information on stopping NTP, see "Stop" (p. 2-11) and "Start" (p. 2-6) . For information on **imp_db** , see "imp_db (and imp_ws) Command" (p. C-10) .

1 Log on the NTP as **ntp** . (You must be logged on as **ntp** to proceed.)

2 Stop NTP by entering **$APPLBIN/ntpstop**

3 Enter **$APPLBIN/imp_db**

Result:

```
The following tables can be recovered individually
SYSTEMINFO, CUSTID, ACASE and VPNID
Do you want to recover any of these tables [y/n];
```

4 Enter **y**

Result: You see the following prompts, one by one:

```
Do you want to recover SYSTEMINFO table [y/n]:
Do you want to recover CUSTID table [y/n]:
Do you want to recover ACASE table [y/n]:
Do you want to recover VPNID table [y/n]:
```

5 Enter **y** or **n** at EACH prompt to select the table(s) you want to recover.

Important! If you also lost working sets, you may want to recover them all now by entering, **imp_ws** . See "Recover Working Sets from $ORAEXPORT" (p. C-24) .

6 Start NTP by entering **$APPLBIN/ntpstart**

END OF STEPS

Recover all BUT systeminfo, custid, acase, or vpnid from $ORAEXPORT

Purpose

Use this procedure to recover all tables BUT the listed tables, from $ORAEXPORT. The procedure requires you to use the **ntpstop** and **ntpstart** commands to stop and restart NTP. For information on stopping NTP, see "Stop" (p. 2-11) and "Start" (p. 2-6) . For information on **imp_db** , see "imp_db (and imp_ws) Command" (p. C-10) .

1 Log on the NTP host as **ntp** . (You must be logged on as **ntp** to proceed.)

2 Shut down NTP by entering: **$APPLBIN/ntpstop**

3 Enter **$APPLBIN/imp_db**

Result:

```
The following tables can be recovered individually
SYSTEMINFO, CUSTID, ACASE and VPNID
Do you want to recover any of these tables [y/n];
```

4 Enter **n**

Result:

```
To recover any other reference table, all the other reference
tables will have to be recovered. Continue with the recover
 [y/n]:
```

5 Enter **y**

Important! If you also lost working sets, you may want to recover them all now by entering, **imp_ws** . See "Recover Working Sets from $ORAEXPORT" (p. C-24) .

6 Start up NTP by entering: **$APPLBIN/ntpstart**

END OF STEPS

Recover all tables from $ORAEXPORT

Purpose

Use this procedure to recover all tables BUT the listed tables, from $ORAEXPORT.

1 Log on as **ntp** .

2 Shut down NTP by entering: **$APPLBIN/ntpstop**

3 Enter **$APPLBIN/imp_db**

Hint: For the **imp_db** *command, see* "exp_db Command" (p. C-8) .

Result:

```
The following tables can be recovered individually
SYSTEMINFO, CUSTID, ACASE and VPNID
Do you want to recover any of these tables [y/n];
```

4 Enter **n**

Result:

```
To recover any other reference table, all the other reference
tables will have to be recovered. Continue with the recover
 [y/n]:
```

5 Enter **n**

Result: `Recover the entire reference database [y/n]:`

6 Enter **y**

Important! If you also lost working sets, you may want to recover them all now by entering, **imp_ws** . See "Recover Working Sets from $ORAEXPORT" (p. C-24) .

7 Start up NTP by entering: **$APPLBIN/ntpstart**

END OF STEPS

Recover Working Sets from $ORAEXPORT

Purpose

The procedures in this section tell how to recover working sets (user files) from $ORAEXPORT to databases.

Background

Working sets are databases created automatically or manually by users:

- *Automatically*. Each time a GUI user uses Find to retrieve data from a database, the retrieved data is saved in a database file called a working set. Each user's automatically created working sets are named ws, ws_prev, ws_view, and ws_view_prev. These overwrite each other with each Find. Typically, these are NOT worth recovering.)
- *Manually*. A user can manually rename an automatically created a working set. It is retained until he or she manually removes it. Since users purposely save these, they may be worth recovering.

Working sets are backed up (along with other databases) by:

- **`exp_db`** — into files in $ORAEXPORT (automatically done daily from **`cron`**)

Before you begin

Working sets are in $ORAEXPORT/DMP/*.ws.dmp where * is the username in uppercase. Check there to make sure the working set files you want exist. If they do not, recover the files from tape.

Recover all working sets from $ORAEXPORT

Purpose

Use this procedure to recover all working sets from $ORAEXPORT to databases.

1 Log on the NTP host as **ntp**. (You must be logged on as NTP to proceed.

2 Enter **$APPLBIN/imp_ws**

END OF STEPS

Appendix D: Set Up 8925 Integrated Service Assurance

Overview

Purpose

The 8925 Integrated Service Assurance system (8925 ISA) collects CIMs from switches and forwards the CIMs to the NTP software system. (8925 ISAs can do other things, but this is all NTP uses them for.)

5ESS, DMS, and 1A *ESS* link administration must be performed by the 8925 ISA administrator while logged on an 8925 ISA machine.

Contents

Introduction

Source

5ESS, DMS, and 1A *ESS* link administration must be performed by the 8925 ISA administrator while logged on an 8925 ISA machine. The procedure for link administration is provided here as a courtesy to help you work with the 8925 ISA administrator to ensure that administration is correctly performed for NTP.

The source for the procedure is the *8925 ISA Administrator Guide*, 190-422-527.

For 8925 ISA and administration you do on the NTP host (such as adding or deleting an 8925 ISA at the host), see " 8925 Integrated Service Assurance Sources" (p. 5-30).

When to use

Typically, 8925 ISA is administered only once for NTP, during NTP installation.

Coordinate

Consult with your NTP support organization before working with the 8925 ISA administrator.

Other terms for 8925 ISA

8925 ISA was formerly known as *Navis*® Network Fault Management system (NFM).

You may see several old terms and other designations that mean 8925 ISA in references, messages, and file or directory names. For a list, see "Other terms for a ISA source" (p. 5-30).

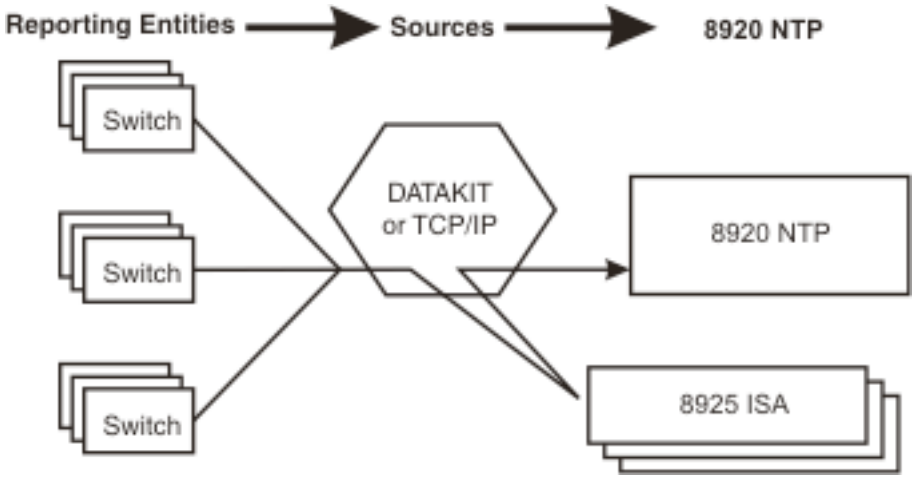
Reference

For general information on CIM I/O with 8925 ISA, see Chapter 5, "CIM Source Administration".

Background

CIMs flow from switches, through 8925 ISA, and to NTP, running on its host computer.

For a list of switches for which 8925 ISA forwards CIMS to NTP, see "Source Types and REs" (p. 5-10).



Purpose

When NTP software is installed, it includes a pattern file to tell 8925 ISA which switch messages to forward to NTP. (There is one pattern file for ALL switch types.) Before the file can be used, the following must occur:

1. *Send the Pattern File.* Use "Send the Pattern File" (p. D-4) to send the pattern file from NTP to 8925 ISA.
2. *Copy the Pattern File.* Ensure that the 8925 ISA administrator uses "Copy the Pattern File" (p. D-5) to copy the pattern file.
3. *Set Up 8925 ISA.* Ensure that the 8925 ISA administrator uses "Set up 8925 ISA" (p. D-6) to tell 8925 ISA to send CIMs to NTP.

   Important! On NTP. You must also use procedures in Chapter 5, "CIM Source Administration" to set up NTP to receive CIMs from 8925 ISA.

Send the Pattern File

Purpose

This procedure sends (or copies) the pattern file from the NTP host machine to an 8925 ISA host machine so that the 8925 ISA administrator can access it.

For how this fits with other procedures, see "Purpose" (p. D-3).

Procedure

Use this procedure to send the pattern file from the NTP host machine to an 8925 ISA host machine:

1 Log on NTP as **`ntp`**. (You must be logged in as **`ntp`** to proceed.)

2 Enter the following to go to the directory where the pattern file, tsm.pat resides:

```
cd $MODELDIR/pat/tsm.pat
```

3 Use ftp (file transfer protocol) or any other utility or tool (such as attaching the file to email) by which you can copy the pattern file from the NTP host to the 8925 ISA host.

Important! To use **`ftp`**, you must have permission to access the 8925 ISA machine.

4 Tell the 8925 ISA administrator where you have copied the file, or how to access it (if you used email).

END OF STEPS

Copy the Pattern File

Purpose

This procedure has the 8925 ISA administrator copy the tsm.pat pattern file to a new filename on the 8925 ISA host.

Important! For how this fits with other procedures, see "Purpose" (p. D-3).

Procedure

Use this procedure to copy the tsm.pat pattern file to a new filename on the 8925 ISA host:

1 Log on the 8925 ISA host as the 8925 ISA administrator.

2 Locate the pattern file sent by the NTP administrator, and copy it to the filename nfm. To do this, enter **`cp tsm.pat nfm`**

3 Make a note of the directory location of the nfm file. You will need this information in "Set up 8925 ISA" (p. D-6).

4 Store the tsm.pat file in case it is needed again.

END OF STEPS

Set up 8925 ISA

Purpose

Have that the 8925 ISA administrator complete this procedure to tell 8925 ISA to forward CIMs to NTP.

For how this fits with other procedures, see "Purpose" (p. D-3) .

Procedure

Complete this procedure to tell 8925 ISA to forward CIMs to NTP:

1 Have the procedures in "Copy the Pattern File" (p. D-5) been completed?

- If YES, go to the next step.
- If NO, go to "Copy the Pattern File" (p. D-5) .

2 Log on 8925 ISA as the 8925 ISA administrator.

Result: A menu similar to the following appears:

```
  COMMAND MENU [ tnm_m ]

cmds   User Commands

osap   OSAP Administration

tim    TIM

nei    NEI Commands

rtn    Return
```

3 Enter **osap** and press **Return** .

Result: A menu similar to the following appears.

```
ADMINISTER OSAP MENU [ admosap_m ]x

port      Port Administration

netp      Network Element Type Administration

ne        Network Element Administration

srctp     Data Source Type Administration

src       Data Source Administration

pat       Pattern Administration

perm      Permission Administration

prntr     Printer Administration

osif      Operations Support Systems Administration

schd      Scheduler Administration

meas      Measurement Administration

sec       Security Administration

lkupadm   Table Lookup Administration

udtr      UDTR Administration

rtn       Return
```

4 Enter **`pat`**

Result: A menu similar to the following appears.

```
ADMINISTER PATTERN MENU [ admpat_m ]

upat    User Pattern Administration

lpat    Logging Pattern Administration

dpat    Data Distributor Pattern Administration

scpat   Sctab Pattern Administration

simpat  Simple Pattern Administration

rtn     Return
```

5 Enter **dpat**

Result: A menu similar to the following appears.

```
ADMINISTER DATA DISTRIBUTOR PATTERN MENU [ admdpat_m ]

view   View Data Distributor Pattern

ed     Edit Data Distributor Pattern

cpy    Copy Data Distributor Pattern

dlt    Delete Data Distributor Pattern

ex     Exercise Data Distributor Pattern

actv   Activate Data Distributor Pattern
```

6 Enter **ed**

Result: A screen appears, similar to the one shown in the next step.

7 Type values on the screen as follows:

```
EDIT DATA DISTRIBUTOR PATTERN [eddpat]

Pattern name: * nfm
 <see note, below
)

Base pattern location <local,cur,prev>: local


Subsystem name:

Base pattern name: <see note, below
>

Data source type: <see note, below
>
```

Please note the following:

- For the entry in the **Pattern name** field, this step assumes "nfm" is the name you gave the pattern file in "Copy the Pattern File" (p. D-5) and that the nfm file is in the current working directory. If it is not, enter the appropriate pathname.
- Use local for the value in the **Base pattern location** field.
- If you do not know the base pattern name, do the following to complete the **Base pattern name** field:
  - Press **Control-Shift-?** to see a dialog box similar to the following to display a list of current base patterns:

    ------ <TEXT> ------
    |---------list-----------|
    |---------rtn-----------|
  - Select **list** in the dialog box to see the list.
  - Select any pattern from the list, and press **Enter** .
- In the **Data source type** field, you can enter ess5, ess1A, ess4, dms100, dms 250, dms500, or another string defined in NTP's eqtype table. The Data source type you specify MUST already be defined as a data source on 8925 ISA.

8 At the last field, press **Return** .

Result: A dialog box similar to the following appears on the same screen:

```
------ CONFIRM -----

|       redo        |

|       exec        |

|       rtn         |

--------------------
```

9 Enter **exec**

Result: You are in a file for editing the base pattern file with the *vi* editor, with your cursor on the first line. The file resembles the following:

```
/*

** This pattern is associated with data source type <ess5>

*/

~

~

"/tmp/EdPat22124.pat" 3 lines, 64 characters
```

10 With your cursor on the first line, edit the file as follows:

1. Delete all lines in the file. To do so, press and release **Escape** and then type:**1,$d**
   (The number **1** signifies the first line in the file, **$** signifies the last line, and **d** means delete.)
2. Read in the 8925 ISA pattern file. To do so, press and release **Escape** and then type
   :**r nfm**
   where nfm is the name you gave the pattern file in "Copy the Pattern File" (p. D-5) .
   (You may need to type a pathname if the file is not in your working directory.)
3. Press and release **Escape** and then enter :**wq**

Result: You write and quit the file. This automatically compiles the nfm file. Then you receive a message confirming compile completed. You may receive a prompt asking if you want to continue. Then you return to the following menu.

```
ADMINISTER DATA DISTRIBUTOR PATTERN MENU [ admdpat_m ]

view   View Data Distributor Pattern

ed     Edit Data Distributor Pattern

cpy    Copy Data Distributor Pattern

dlt    Delete Data Distributor Pattern

ex     Exercise Data Distributor Pattern

actv   Activate Data Distributor Pattern
```

11 Enter **actv**

Result: A screen appears, similar to the one shown in the next step.

12 Enter the values shown in bold as follows and then press **Return** .

```
ACTIVATE DATA DISTRIBUTOR PATTERN [actvdpat]

Pattern location <local,prev>:* local


               Subsystem name:* osif


               Pattern name:* nfm
```

Result: The following message appears:

```
Your pattern is activated.
```

13 Press and release **Escape** , and type **home** , and press **Return** .

Result: You return to this menu:

```
    TNM MENU [ tnm_m ]

cmds  User Commands

osap  OSAP Administration

tim   TIM

nei   NEI Commands

rtn   Return
```

14 Enter **osap**

Result: A menu similar to the following appears:

```
ADMINISTER OSAP MENU [ admosap_m ]x

port      Port Administration

netp      Network Element Type Administration

ne        Network Element Administration

srctp     Data Source Type Administration

src       Data Source Administration

pat       Pattern Administration

perm      Permission Administration

prntr     Printer Administration

osif      Operations Support Systems Administration

schd      Scheduler Administration

meas      Measurement Administration

sec       Security Administration

lkupadm   Table Lookup Administration

udtr      UDTR Administration

rtn       Return
```

15 Enter **`osif`**

Result: A menu similar to the following appear:

```
ADMINISTER OPERATIONS SUPPORT SYSTEMS (OS) DATA MENU [ admosif_m ] x

 viewosdata  View OS Data

  dfnosdata  Define OS Data

  updosdata  Update OS Data

  dltosdata  Delete OS Data

 actvosdata  Activate OS Data

dactvosdata  Deactivate OS Data

  viewsrcos  View OS/DataSource Association

   dfnsrcos  Define OS/DataSource Association

   dltsrcos  Delete OS/DataSource Association

        rtn  Return
```

16 Enter **dfnosdata**

Result: A screen appears, similar to the one shown in the next step.

17 Enter values shown in bold below:

```
DEFINE OS DATA [dfnosdata]

OS name:* ntp

Distributor pat name: 1

OS type:* udos

Activate <y,n>: y

message type(s):* status,drsc,wdog,file

OS baud rate: 9600

Transmission type: priv

Back-up baud:

Telephone number:

Printer type:

Back-up phone number:

Start of message:

Port name: >

End of message:

Back-up port name:

Scheduler time:

Reformatting pat name:

2nd Scheduler time:

Define UDOS message header <n,y>: y
```

18 Still on the same screen in *Step 17* , press **Return** until you come to the Port name: field. The following window pops up:

```
DEFINE PORT DATA [ dfnport ]

              Port name:* <see note, below>

           Port function:* osif

            Network type:* <see note, below>

                 Address: <see note, below>

            Port Options: <leave blank>
```

Please note the following:

- In the Port name: field, enter any name you want to assign to the port, such as ntp1.
- In the Network type: field, enter **enet** (for ethernet or TCP/IP), **int** (for internal) or **dk** (for *Datakit*). (NOC1 uses TCP/IP only. 8925 ISA can use *Datakit* or TCP/IP.)
- In the Address: field, enter the NTP system name and port as assigned by the NTP administrator. This address must be defined in the */etc/hosts file* as *IP_address-:port_id* . Example: netntp:3000

19 At the last field press **Return** .

Result: A dialogue box similar to the following appears:

```
------ CONFIRM -----

|       redo       |

|       exec       |

|       rtn        |

--------------------
```

20 Enter **`exec`**

Result: You return to the screen in *Step 17* . The Port name: field is filled in.

21 Still on the same screen in *Step 17* :

1. Press **Return** until you come to the "Start of message field". Press **CONTROL-?** (simultaneously press the **CONTROL** and **?** keys) to call up a help window. Use that window to enter **`/001`**
   (This represents **Control-A** .)
2. Press **Return** until you come to the "End of message field". Press **Control-?** (simultaneously press the **Control** and **?** keys) to call up a help window. Use that window to enter **`/003`**
   (This represents **Control-C** .)

   Result: You return to the screen in *Step 17* . The "Start of message field" the "End of message field" are filled in.

22 Still on the same screen in *Step 17* , press **Return** until you come to the "Define UDOS message header <n,y>" field and enter **`y`**

Important! Use **`clli`** if the switch is defined as Ne and the CLLI code is complete. Otherwise, instead of **`clli`** for the network element CLLI, you can use **`srcname`** for the data source name. (See *Step 28* .)

Result: The following window pops up. Fill in the two fields shown in bold below:

```
DEFINE UDOS MESSAGE HEADER [udoshdr]

FIELD    TYPE     CONTENTS              FIELD TYPE CONTENTS

1:       ttype
                              9.

2:       clli <see note below>
      10.

3:                                        11.
```

23 At the last field press **Return** .

Result: A dialogue box similar to the following appears:

```
------ CONFIRM -----

|       redo       |

|       exec       |

|       rtn        |

--------------------
```

24 Enter **exec**

Important! For the Port name: field, see *Step 17* .

Result: You return to the screen in *Step 17* . The screen should now resemble the following:

```
DEFINE OS DATA [dfnosdata]

OS name:* ntp


Distributor pat name: nfm


OS type:* udos


Activate <y,n>: y


message type(s):* status,drsc,wdog,file


OS baud rate: 9600


Transmission type: priv


Back-up baud:

Telephone number:

Printer type:

Back-up phone number:

Start of message:/001


Port name: ntp1


End of message:/003


Back-up port name:                          S

cheduler time:
```

```
Reformatting pat name:

2nd Scheduler time:

Define UDOS message header <n,y>: y
```

25 With your cursor on the last field, press **Return** .

Result: A dialogue box similar to the following appears on the same screen:

```
------ CONFIRM -----

|       redo       |

|       exec       |

|       rtn        |

--------------------
```

26 Enter **exec**

Result: You return to the same screen.

27 Press and release **Escape** and then type **dfnsrcos**

Result: A screen appears, similar to the one shown in *Step 28* .

28 Enter values shown in bold.

```
DEFINE OS - DATA SOURCE ASSOCIATION [dfnsrcos]

   Data source name:* <source — see note, below>


            OS name:* ntp
```

Important! Data source name is whatever 8925 ISA name you gave to the network element.

Result: A dialogue box similar to the following appears on the same screen:

```
------ CONFIRM -----

|        redo        |

|        exec        |

|        rtn         |

--------------------
```

29 Enter **exec**

Result: You return to the previous screen.

30 Exit 8925 ISA.

END OF STEPS

Change 8925 ISA

See your support organization

To change a pattern file in order to change which switch messages are collected and forward to NTP, see your NTP support organization.

Such changes would require changing not only the pattern file, but also NTP code.

Appendix E: CFIM Field-to-PCMD, MTX, Autoplex and Sonus Data Mapping

Overview

Purpose

The tables in this appendix map values found in the CFIM table to the PCMD, MTX, Autoplex and Sonus-specific data interpretation from the PCMD, MTX, Autoplex and Sonus GSX records.

Example: If the caus field of the CFIM table contains a value of 2, refer to the table "PCMD Mapping for CFIM caus field" (p. E-4). There you will find that a value of 2 in this field corresponds to a PCMD record meaning of "Call unanswered and ended normally."

PCMD Converter

The Per Call Measurement Data (PCMD) converter provides the means to collect, parse, interpret, expand, store and analyze PCMD records from *Autoplex*. PCMD records are detailed call records produced for each call, and contain information regarding the call setup, components used on the call, call disposition, performance metrics, and other call attributes.

EvDO PCMD information

EvDO (Evolution - Data Only) is a wireless broadband technology used with the CDMA (Call Division Multiple Access) technology. EvDO PCMD records are obtained from the OMP (Operations and Management Platform) in a Lucent EvDO network, and then converted to messages that allow NTP users to detect and analyze problems in a EvDO 3G network.

The table related to EvDO PCMD (p. "EvDO PCMD Mapping for CFIM sm_cnt1-sm_cnt15 fields" (p. E-23)) in this appendix maps values found in the CFIM sm_cnt1-sm_cnt15 fields to their corresponding meanings in the EvDO PCMD record.

CDMA Call Data Geolocation

This feature provides for the geolocating of CDMA call records to identify the location of each call.

Each CFIM record is populated with the following data:

- longitude,
- latitude,
- computation probability of the location,
- PCMD change of access and ending carrier, and
- PSMM change of access and ending carrier.

The feature is built on a current capability of NTP to collect PCMD PSMMs (Pilot Strength Measurement Messages) produced by Lucent Flexent/Autoplex wireless switches, allowing NTP users to do detailed analysis of the radio frequency (RF) conditions at the end of each call that was assigned a traffic channel.

Sonus Converter

The Sonus converter provides the means to collect, parse, interpret, expand, store and analyze Sonus Attempt and Sonus Stop records from the Sonus GSX9000 and GSX4000 Open Services Switches.

Attempt records are used as traditional call irregularity messages (CIMs) to do call failure analysis in the VOIP network. The data from these records also enables analysis that is expanded to the ingress and egress network elements, providing a complete end-to-end picture.

Stop records are used for billing, and they contain QOS parameters that can be used to determine whether the quality of a call is acceptable.

Contents

PCMD Mapping for CFIM caus field

Purpose

This table maps values found in the CFIM caus field to the corresponding meaning in the PCMD record.

The caus field describes the protocol failure that occurred when the call CIM was created at the Reporting Entity.

Value	Qualifier	Additional Information
1	Call answered and ended normally	
2	Call unanswered and ended normally	The calling party hung up.
3	Called party was busy	The called mobile was busy. The secondary qualifier indicates whether the call was routed to voicemail.
4	Unanswered call (alert timeout) from cell	The called mobile did not answer prior to alert time-out. The secondary qualifier indicates whether the call was routed to voicemail.
5	Handoff to another MSC	An inter-MSC handoff occurred
6	Reacquired on analog	An analog-capable mobile was reacquired on analog, probably because of a lack of available CDMA channels.
7	Termination abandon	A terminating mobile is assigned this CFCQ when the calling party releases before the call is answered.
8	No page response	The called mobile did not respond to the paging attempts. The secondary qualifier indicates whether the call was routed to vicennial.
9	Inter-DCS hard handcuff to analog	An inter-DCS hard handoff to analog occurred.
10	Soft handoff to another DCS	A soft handoff to another DCS occurred.
11	Concurrent feature activation completed	A feature activation code was entered during a stable call.
12	SMS call on Idle Traffic channel	COTRAF - IDLE, CTRAF - IDLE
13	SMS call on Busy Traffic channel	COTRAF - BUSY, CTRAF - BUSY No SMS calls set up on a busy traffic channel are assigned a CFC of 2-13.

Value	Qualifier	Additional Information
14	SMS call on Paging channel	CPAGE No SMS calls set up on a busy paging channel are assigned a CFC of 2-13.
15	SMS call on Access channel	COACC No SMS calls set up on a access channel are assigned a CFC of 2-13.
16	Tandem call	Creates a per-call data record for tandem-only leg.
17	Hard handoff to analog	An intra-MSC hard handoff to analog has occurred with the call.
18	RLP Timeout	The call was complete due to RLP timeout
21	RP_CLOSED	The call ended normally due to RLP or PCF connection begin closed
22	Mobile Inactivity Timeout	The terminating mobile is inactive and the MSC does not send a page.
23	Called party mobile was inactive	The terminating mobile is inactive and the MSC does not send a page.
100	Dropped call	The call was dropped after traffic channel confirmation and the call was stable on the radio channel and the packet pipe connection had been established. This CFCQ is assigned for system-initiated events only if the call was torn down for reasons not related to a release from either the mobile or the network, and is mutually exclusive with a Lost Call condition. The secondary qualifier indicates whether the call was dropped "After Traffic Channel Confirmation/Before Answer or After Answer."
101	Mobile powered down	The call was dropped due to a non-user initiated power down, for example, the mobile's battery died.
102	Packet pipe disconnect	The call was dropped due to a loss of communication on the packet pipe between the cell and the DCS.
103	Cell Stable Clear	The call was torn down due to a stable clear initialization event at the cell.
104	Cell shutdown - handoff complete timeout	The call was torn down due to the cell shutting down the call due to a handoff complete timeout.
105	DCS Failure	The call was dropped due to a failure reported by the DCS. There are a variety of potential failure reasons that could cause this situation.

Value	Qualifier	Additional Information
106	Lost Call	This CFCQ is assigned when the cell detects a loss of continuity in traffic going from the mobile to the cell site. This loss could be the result of mobile equipment problems or, most likely, RF coverage limitations.
107	Zero pre-pay account balance	The call was torn down when the balance on the pre-paid account went to zero during the call.
108	Speech handler protocol failure	The call was torn down because of a communication protocol failure between the cell and the speech handler in the DCS.
109	Release Confirmation Failure	The call was considered dropped because the mobile did not confirm the release order.
110	Manual Termination	An existing call is manually terminated by a switch command or automatically terminated by an audit.
111	Misc. Drop	The call was dropped but a specific reason was not determined.
112	Bearer Path Failure at RNC	The call was dropped due to Bearer Path Failure from the RNC.
113	Call Ended	The call ended because of redirection during IBLM feature execution for mobile origination scenario.
200	Origination inhibited	The Origination Major Class field, located in the subscriber database, for this subscriber, indicates that the attempt should be inhibited.
201	ESN mismatch (Fraud)	The mobile serial number is either in the fraud database or is otherwise not validated.
202	Stolen Mobile	The mobile is marked as stolen in the subscriber database.
203	Roamer attempt denied	The subscriber is not authorized for roaming.
204	Zero pre-pay account balance	The subscriber has a pre-pay balance of zero.
205	Unassigned number	The number is not allocated in the subscriber database.
206	Misdialed number	An attempt to interpret the originating digits has failed in digit analysis.
300	Termination Inhibited	The Termination Major Class field, located in the subscriber database, for this subscriber, indicates that the attempt should be inhibited.
301	ESN mismatch (Fraud)	The mobile serial number is either in the fraud database or is otherwise not validated.

Value	Qualifier	Additional Information
302	Stolen Mobile	Terminations to stolen mobiles are generally not inhibited. This qualifier tracks accesses to Remote Feature Activation (RFA) where a subscriber dials a special DN to initiate an RFA.
303	Roamer attempt denied	The subscriber is not authorized for roaming.
304	Zero pre-pay account balance	The subscriber has a pre-pay balance of zero.
305	Unassigned number	The number is not allocated in the subscriber database
401	ECP-related failure	Failure was due to an internal ECP software problem, for exa.mple, database error or expired timers.
402	Unauthorized 3G HSPD attempt	An unauthorized 3G HSPD attempt is one from a mobile unit that is not provisioned (i.e. authorized) to use 3G HSPD service.
403	Call failure due to database failure	An ECP-related database failure has occurred, causing the call to fail.
404	Secondary treatment failure/blocking	For a terminating call, if a miscellaneous failure is detected at the ECP, the system tries the secondary treatment such as call forwarding or MRS for the mobile. For reasons such as subscriber configuratino or system restriction, the secondary treatment is failure/blocking.
500	No idle speech handlers	The call was blocked because of a lack of available speech handlers of the correct type in the DCS.
501	Speech handler request failure	The call failed because the ECP request to the DCS for a speech handler failed.
502	Speech handler activation failure	Speech handler activation failureA speech handler was successfully assigned to the call but the speech handler failed the hardware activation needed to serve the call.
503	Speech handler protocol failure	There was a protocol error between the cell and the allocated speech handler.
504	Speech handler - packet pipe frame connectivity error	There was a packet pipe frame connectivity error between the cell and the allocated speech handler.
505	Packet pipe connection failure	The call failed because of a DCS-to-cell packet pipe communication failure.
506	Service option rejected	The call was blocked due to the lack of a compatible speech handler.
507	DCS network blocked	The call failed due to blocking within the DCS itself.

Value	Qualifier	Additional Information
508	Remote trunk congestion	The call failed because all acceptable trunks from the DCS were blocked.
509	PSTN Data Path (PDP) setup failure	A data-call-specific setup failure occurred.
510	Other DCS/Network failure	This CFCQ is assigned for a variety of reasons; a more specific reason is undetermined.
600	Traffic channel confirmation failure	The call failed because the cell did not receive acknowledgement from the mobile that the mobile had successfully established the air interface link.
601	Traffic channel activation failure	The call failed due the traffic channel element failing a hardware activation needed to serve the call.
602	Traffic channel unavailable	The call was blocked due to the lack of a suitable traffic channel to serve the call.
603	Packet pipe blocked	The call was blocked due to the lack of packet pipe capacity needed to complete the connection to the DCS.
604	Walsh code unavailable	An overflow CFCQ for this CFC is assigned based on the blockage condition encountered on the first carrier tried by the channel element allocation algorithm.
605	Back-haul server blocked	Congestion in the IP back-haul server has caused the call to be blocked.
606	Power control overload	The call was blocked due to the lack of forward or reverse link power to needed to complete the connection to the mobile unit.
607	No speech handler assigned	The call failed because the cell did not receive the information about the assigned speech handler from the DCS.
608	Alert confirmation failure	The call failed because the mobile did not acknowledge the alerting message from the cell, probably due to an RF coverage issue.
609	Internal cell processing error	This CFCQ is assigned for a variety of reasons; a more specific reason is undetermined.
610	Multi-link Group blocked	Congestion on the multi-link group has caused the call to be blocked.
611	Origination SO renegotiation from EVRC-B to EVRC has failed	This CFCQ takes precedence over other CFCQs that may also be pegged when renegotiation fails.

Value	Qualifier	Additional Information
700	SMS Network resource Shortage	SMS Cause Code 2. General Resource failure/time-out.
701	Invalid Teleservice ID	SMS Cause Code 4. Unknown/unsupported teleservice ID.
702	Mobile Not Found	SMS Cause Codes 32 and 38. No page response or terminal no longer there.
703	SMS Delivery Postponed	SMS Cause Code 36. Delivery postponed.
704	SMS Service not supported	SMS Cause Codes 97, 98, 100. Attempt denied due to subscriber denied or service provisioning error.
705	Other SMS Failure	SMS failure due to a variety of reasons; a more specific reason is undetermined.
1503	Internal RNC Communications Failure	There was an internal RNC failure due to communications problems with the TPU shelf or the PCF.
1504	No FSRM Available	No FSRM available
1505	TP Request Failure	The TP request has failed due to PCF unable to take calls due to overload, the TCS AP'S CPU was in over load or for other reasons.
1507	TP Protocol failure	TP protocol failure due to the interface between the TPU and the TCS or the TCS and the RCS.
1704	A10/A11 Failure	This failure occurs when PCF resources are unavailable or there's a PDSN failure.

PCMD Mapping for CFIM caus2 field

Purpose

This table maps values found in the CFIM caus2 field to the corresponding meaning in the PCMD record.

The caus2 field provides additional failure information from the reporting entity.

Value	Secondary Qualifier
0	Not redirected to voicemail
1	Redirected to voicemail
2	Forward link power control overload (caus=606 only)
2	After TC CONF, Before Answer
3	Reverse link power control overload (caus=606 only)
3	After Answer

PCMD Mapping for CFIM ct field

Purpose

This table maps values found in the CFIM ct field to the corresponding meaning in the PCMD record.

The call type (ct) field describes the type of call involved.

Value	Call Processing Type
1	Freeland
2	Local operator used
3	Local
4	Toll
5	IDDD
6	Termination
7	Mobile
8	Immediate CF activation
9	Conditional CF activation
10	ICF deactivation
11	CCF deactivation
12	All CF deactivation
13	Security entry
14	Toll operator used
18	Special routing (de)activation
19	Intra-circle cellular-originated call
21	VMSS MRS (de)activation
24	Unknown act/deactivation
25	CN-II term slave
27	CN-II handoff
31	SALSA (de)activation
33	MCCPE activation
34	PIN activation
35	Do not disturb (MAS)
37	SPINA (de)activation

Value	Call Processing Type
39	CCF split busy (de)act
41	CCF split no reply (de)act
43	NPNI user zone activation
44	NPNI user zone tone deactivation
47	Mobile status trigger deactivation
52	Flexible alerting activation
53	Flexible alerting deactivation
54	Preferred language
55	Call transfer activation
56	Call transfer deactivation
57	DOCR activation
58	Mobile-originated call failed or blocked before traffic channel assignment
59	Mobile-terminated call failed or blocked before traffic channel assignment
62	CFD Activation
63	CFD Deactivation

PCMD Mapping for CFIM req_st field

Purpose

This table maps values found in the CFIM req_st field to the corresponding meaning in the PCMD record.

This field provides information about the Requested Service Type.

Value	Service Option
0	unknown option
1	8K Voice
2	8K Mobile Loop Back Test
3	EVRC 8K Voice
4	9.6K Async Data
5	9.6K Fax - Digital fax
6	Short Message Service
7	Packet data 9.6 IP service
9	13K Mobile Loop back Test - CDMA Mobile Loop back Test (13K Vocoder)
12	14.4K Async Data
13	14.4K FAX - Digital fax
14	13K Short Message Service
15	Packet data 14.4 IP service
17	13K Voice (Official Service Option Number assigned by standard body to replace 32768)
20	9.6K Analog Fax Service
21	14.4K Analog Fax Service
33	Packet Data 3G - 1X IP Service
56	SMV voice service
32768	13K Voice (Proprietary Service Option Number assigned to Qualcomm Vocoder)
32799	13K Markov
32770	8K Markov - Markov Test (for CDMA, between Mobile and Channel Element)
32798	8K Markov

PCMD Mapping for CFIM st field

Purpose

This table maps values found in the CFIM st field to the corresponding meaning in the PCMD record.

The service type (st) field describes the type of service involved in the CIM.

Value	Service Option
0	unknown option
1	8K Voice
2	8K Mobile Loop Back Test
3	EVRC 8K Voice
4	9.6K Async Data
5	9.6K Fax - Digital fax
6	Short Message Service
7	Packet data 9.6 IP service
9	13K Mobile Loop back Test - CDMA Mobile Loop back Test (13K Vocoder)
12	14.4K Async Data
13	14.4K FAX - Digital fax
14	13K Short Message Service
15	Packet data 14.4 IP service
17	13K Voice (Official Service Option Number assigned by standard body to replace 32768)
20	9.6K Analog Fax Service
21	14.4K Analog Fax Service
33	Packet Data 3G - 1X IP Service
56	SMV voice service
32768	13K Voice (Proprietary Service Option Number assigned to Qualcomm Vocoder)
32799	13K Markov
32770	8K Markov - Markov Test (for CDMA, between Mobile and Channel Element)
32798	8K Markov

PCMD Mapping for CFIM sm_cnt1-sm_cnt10 fields

Purpose

This table maps values found in the CFIM sm_cnt1-sm_cnt10 fields to their corresponding meanings in the PCMD record.

The sm_cnt1-sm_cnt10 fields provide Service Measurement (sm) information.

Value	Count Group	SM Number	SM Count Name
01	ECP-PAF-CARR-SC CDMA	3 (2G), 14 (3G)	Origination Traffic Channel Confirmation Failure
02	ECP-PAF-CARR-SC CDMA	4 (2G), 15 (3G)	Termination Traffic Channel Confirmation Failure
03	ECP-PAF-CARR-SC CDMA	5 (2G), 18 (3G)	Origination Traffic Channel Activation Failure
04	ECP-PAF-CARR-SC CDMA	6 (2G), 19 (3G)	Termination Traffic Channel Activation Failure
05	ECP-PAF-CARR-SC CDMA	1 (2G), 16 (3G)	Origination Denied due to No Packet Pipe (PP) Connection
06	ECP-PAF-CARR-SC CDMA	2 (2G), 17 (3G)	Termination Denied due to No PP Connection
07	ECP-PAF-CARR-SC CDMA	24 (2G), 26 (3G)	Origination Failed due to No Speech Handler Assignment Received at Cell
08	ECP-PAF-CARR-SC CDMA	25 (2G), 27 (3G)	Termination Failed due to No Speech Handler Assignment Received at Cell
09	ECP-PAF-CARR CDMA	11 (2G), 14 (3G)	Page Response Seizures due to Silent Page
10	ECP-PAF-CARR CDMA	12 (2G), 15 (3G)	Page Response Seizures Not Resulting in Channel Element (CE) Assignment
11	ECP-PAF-CARR CDMA	1	Origination Denied Due to Power Control Budget
12	ECP-PAF-CARR CDMA	2	Termination Denied Due to Power Control Budget
13	ECP-PAF-CARR CDMA	16 (2G), 18 (3G)	Origination Failed due to DCS Error
14	ECP-PAF-CARR CDMA	17 (2G), 19 (3G)	Termination Failed due to DCS Error

Value	Count Group	SM Number	SM Count Name
15	ECP-PAF CDMA	7 (2G), 10 (3G)	Call Dropped During Talk State due to DCS Error
16	ECP-PAF CDMA	1	Originations Denied due to Traffic Channel not Available
17	ECP-PAF CDMA	2	Terminations Denied due to Traffic Channel not Available
18	ECP-PAF-CARR-SC CDMA	12 (2G), 20 (3G)	Alert Confirmation Failure
19	ECP-PAF CDMA	20 (2G), 22 (3G)	Origination/Termination Reacquired on Analog from CDMA
20	CP-CDMA	18 (2G), 60 (3G)	Originations Denied - Error
21	CP-CDMA	16 (2G), 59 (3G)	Roamer Origination Attempts Denied
22	CP-CDMA	22	Origination Blocked on Outgoing trunk
23	CP-CDMA	21	Origination Network Blocked
24	CP-CDMA	28	Incoming Network Blocking
25	CDMA-PAF-CARR-SC	23 (2G), 36 (3G)	Origination Seizures
26	CDMA-PAF-CARR-SC	24 (2G),37 (3G)	Page Response Seizures
27	CDMA-PAF-CARR-SC	19 (2G), 32 (3G)	Originations Assigned to a Traffic Channel
28	CDMA-PAF-CARR-SC	20 (2G), 33 (3G)	Terminations Assigned to a Traffic Channel
29	CDMA-PAF-CARR-SC	15 (2G), 38 (3G)	CP Fail Call Setup Failure - Origination
30	CDMA-PAF-CARR-SC	16 (2G), 39 (3G)	CP Fail Call Setup Failure - Termination
31	CDMA-PAF-CARR-SC	17 (2G), 40 (3G)	CP Fail Dropped Call
32	CDMA-PAF-CARR-SC	18 (2G), 41 (3G)	Lost Calls
33	CDMA-CARR	2 (2G), 5 (3G)	Origination/Termination Overflow (Channel Element)
34	CDMA-CARR CDMA-SUBCELL	3 3	Origination/Termination Overflow due to Packet Pipe Blocking
35	CDMA-PAF	25 (2G), 60 (3G)	Intercept Message

Value	Count Group	SM Number	SM Count Name
36	CDMA-PAF-CARR-SC	35	2G Originations Assigned to a 3G Channel in 2G Mode
38	CDMA-PAF-CARR-SC	42	3G Originations Assigned to a 2G Channel - CE Overflow
39	CDMA-PAF-CARR-SC	44	3G Originations Assigned to a 2G Channel - PP Overflow
40	CDMA-PAF-CARR-SC	46	3G Originations Assigned to a 2G Channel - RF Balancing
41	CDMA-PAF-CARR-SC	43	3G Terminations Assigned to a 2G Channel - CE Overflow
42	CDMA-PAF-CARR-SC	45	3G Terminations Assigned to a 2G Channel - PP Overflow
43	CDMA-PAF-CARR-SC	47	3G Terminations Assigned to a 2G Channel - RF Balancing
44	CDMA-CARR	6	3G-only Mobile Origination/ Termination Overflow
45	CDMA-PAF-CARR-SC	68	2G Origination Service Connect Complete
46	CDMA-PAF-CARR-SC	69	2G Termination Service Connect Complete
47	CDMA-PAF-CARR-SC	70	3G Origination Service Connect Complete
48	CDMA-PAF-CARR-SC	71	3G Termination Service Connect Complete
49	CDMA-PAF-CARR-SC	120	2G Release Confirmation Failure
50	CDMA-PAF-CARR-SC	121	2G Release Confirmation Failure - Traffic Channel Supervision Interval timer active
51	CDMA-PAF-CARR-SC	122	3G Release Confirmation Failure
52	CDMA-PAF-CARR-SC	123	3G Release Confirmation Failure - Traffic Channel Supervision Interval timer active
53	CDMA-PAF-CARR	185	3G Call Demoted to 2G - RF Capacity
54	CDMA-PAF-CARR	186	3G Call Demoted to 2G - Channel Element Blocking

Value	Count Group	SM Number	SM Count Name
55	CDMA-PAF-CARR	187	3G Call Demoted to 2G - Walsh Code Blocking
56	CDMA-PAF-CARR	188	3G Call Demoted to 2G - Packet Pipe Blocking
57	CDMA-PAF	72	3G Packet Data Origination Blocked - No 3G Cell Resources
58	CDMA-PAF	73	3G Packet Data Termination Blocked - No 3G Cell Resources
59	CDMA-PAF-CARR-SC	154	2G Termination Inter-MSC TLDN Timeout
60	CDMA-PAF-CARR-SC	155	3G Termination Inter-MSC TLDN Timeout
61	CP CDMA	64	New origination attempts from DCS homed cells allocated to RNC
62	CP CDMA	70	Mobile initiated data reactivation requests allocated at RNC without RNC transfer
63	CP CDMA	75	Pakcet Corer new origination attempts sent to DCS - RNC OOS.
64	CP CDMA	77	Data reactivation requests failed - RNC OOS
65	RNC	7	network initiated data reactivation requests allocated at RNC without RNC transfer
66	RNC	9	Mobile Initiated Data Reactivation Attempts with Packet Data Session at RNC Sent to DCS - RNC OOS
67	RNC	10	Network Initiated Data Reactivation Attempts with Packet Data Session at RNC Sent to DCS - RNC OOS
68	RNC	11	Number of Calls Routed to Alternate RNCs
69	CP CDMA	66	Mobile initiated data reactivation requests at RNC
70	CP CDMA	68	r mobile initiated data reactivation requests at RNC with RNC transfer

Value	Count Group	SM Number	SM Count Name
71	CP CDMA	72	mobile initiated data reactivation requests allocated at RNC with RNC transfer
72	RNC	5	network initiated data reactivation requests at RNC
73	RNC	6	network initiated data reactivation requests at RNC with RNC transfer
74	RNC	8	network initiated data reactivation requests allocated at RNC with RNC transfer

PCMD Mapping for CFIM tc field

Purpose

This table maps values found in the CFIM tc field to their corresponding meanings in the PCMD record.

The trouble category (tc) field is used to categorize FDCs.

Value	CFC	Additional Information
1	normal call	The call ended without any failure conditions.
2	dropped call	The call attempt was completed but then was dropped or lost.
3	origination failed - subscriber	The mobile origination attempt was unsuccessful due to a problem with the subscriber's account, mobile unit, or dialing.
4	termination failed - subscriber	The mobile termination attempt was unsuccessful due to a problem with the subscriber's account or mobile unit.
5	origination failed - ECP	The mobile origination attempt failed due to an ECP-related error.
6	termination failed - ECP	The mobile termination attempt failed due to an ECP-related error.
7	origination failed - DCS/network	The mobile origination attempt failed due to a DCS or network-related error or blockage.
8	termination failed - DCS/network	The mobile termination attempt failed due to a DCS or network-related error or blockage.
9	origination failed - cell	The mobile origination attempt failed due to a cell-related error or blockage.
10	termination failed - cell	The mobile termination attempt failed due to a cell-related error or blockage.
11	origination failed - network element independent	The mobile origination attempt failed and the exact cause was undetermined.
12	termination failed - network element independent	The mobile termination attempt failed and the exact cause was undetermined.
13	call failed - network element independent	The call attempt failed. The call type and exact cause were undetermined.

Value	CFC	Additional Information
14	Short Message Service (SMS)	All Short Message Service calls are assigned this value.
15	Origination failed due to RNC	The mobile origination attempt failed due to an RNC related error.
16	Termination failed due to RNC	The mobile termination attempt failed to an RNC related error.
17	origination failed —network/PCF	The origination attempt failed due to a network – or PCF-related error or blockage.
18	termination failed —network/PCF	The termination attempt failed due to a network- or PCF-related error or blockage.
19	Normal ANSI 41 Call Delivery	This CFC only applies to IMC PCMD records.
20	Outbound Call Failure	This CFC only applies to IMC PCMD records.
21	ANSI 41 Signaling Failure	This CFC only applies to IMC PCMD records
22	Abandoned Calls	This CFC only applies to IMC PCMD records.

PCMD Mapping for CFIM silent_reorig field

Purpose

This table maps values found in the CFIM silent_reorig field to the corresponding meaning in the PCMD record.

The silent_reorig field indicates the call record as a normal call or a silent reorigination call and whether it is successful or not.

Value	Call Processing Type
0	For the first call without silent retry.
1	For the failed first call with silent retry.
2	For the successful first call with silent retry.
3	For the failed silent retry call.
4	For the successful silent retry call.

EvDO PCMD Mapping for CFIM sm_cnt1-sm_cnt15 fields

Purpose

This table maps values found in the CFIM sm_cnt1-sm_cnt15 fields to their corresponding meanings in the EvDO PCMD record.

Value	Count Group	SM COUNT DESCRIPTION
01	AN_INIT_CONN_ATT_FAIL _CONFIG_NEGO_FAILED	AN-initiated Connection attempt failures - negotiation fail
02	AN_INIT_CONN_ATTMPT_FAIL_ NO_TCC_RCVD	AN-initiated Connection attempt failures - no response to traffic channel assignment traffic channel confirmation received
03	AN_INIT_CONN_ATTMPT_FAIL_ RL_NOT_ACQ	AN-initiated Connection attempt failures - rev link not acquired
04	AN_INIT_CONN_ATTMPT_FAIL_ NO_RES_AVLBL	AN-initiated connection attempt failures - no resources available
05	AN_INIT_CONN_ATMPT_FAIL_ OTHER_PRETCA	AN-initiated Connection attempt failures - other failures pre TCA
06	AN_INIT_CONN_ATMPT_FAIL_ OTHER_POSTTCA	AN-initiated Connection attempt failures - other failures pre TCA
07	AT_INIT_CONN_ATT_FAIL_ CONFIG_NEGO_FAILED	AT-initiated Connection attempt failures - negotiation fail
08	AT_INIT_CONN_ATTMPT_FAIL_ NO_TCC_RCVD	AT-initiated Connection attempt failures - no traffic channel confirmation received response to traffic channel assignment
09	AT_INIT_CONN_ATTMPT_FAIL_ RL_NOT_ACQ	AT-initiated Connection attempt failures - rev link not acquired
10	AT_INIT_CONN_ATTMPT_FAIL_ NO_RES_AVLBL	AT-initiated connection attempt failures - no resources available
11	AT_INIT_CONN_ATMPT_FAIL_ OTHER_PRETCA	AT-initiated Connection attempt failures - other failures Pre TCA
12	AT_INIT_CONN_ATMPT_FAIL_ OTHER_POSTTCA	AT-initiated Connection attempt failures - other failures Post TCA
13	FAST_CONNECT	Number of fast connection requests
14	RESERVED_14	reserved
15	FAST_CONNECT_FAIL_NO_TCC_ RCVD	Number of fast connection attempt failures due to no Traffic Channel Confirmation received

Value	Count Group	SM COUNT DESCRIPTION
16	FAST_CONNECT_FAIL_NO_RL_ACQ	Number of fast connection attempt failures due to no reverse link being acquired
17	AN_INIT_CONN_REQ	AN-Initiated Connection Requests
18	TCA_FOR_AN_INIT_CONN_REQ	Traffic Channel Assignments for AN Initiated Connection Request
19	AT_INIT_CONN_REQ	AT Initiated Connection Requests
20	TCA_FOR_AT_INIT_CONN_REQ	Traffic Channel Assignments for AT Initiated Connection Requests
21	CONN_REL_RLL	Connection Release - RF Link Lost
22	CONN_REL_OTHER_REASON	Connection Release - Other Reasons
23	RESERVED_23	reserved
24	RESERVED_24	reserved
25	RESERVED_25	reserved
26	RESERVED_26	reserved
27	RESERVED_27	reserved
28	INT_SUBNET_IDL_TRFR_ATTMT	Number of Inter Subnet Idle Transfer Attempts
29	PERS_SWTCH_CONN_TCA	Traffic Channel Assignments for Personality Switch
30	PERS_SWTCH_CONN_ESTABLISHED	Established Connections for Personality Switch
31	CONN_SETUP_PERS_SWTCH_UNKNOWN_TO_REVA	Personality Switches During Connection Setup from Unknown to Rev A
32	CONN_SETUP_PERS_SWTCH_REL0_TO_REVA	Personality Switches During Connection Setup from Rel 0 to Rev A
33	CONN_SETUP_PERS_SWTCH_REVA_TO_REL0	Personality Switches During Connection Setup from Rev A to Rel 0
34	AHO_PERS_SWTCH_REVA_TO_REL0	Personality Switch During Active Connections from Rev A to Rel 0
35	RAN_AUTH_TOTAL_ATTMPT	RAN Authentications – Total Attempts
36	RAN_AUTH_SUCCESSFUL_ATTMPT	RAN Authentications – Successful Attempts
37	RAN_AUTH_FAIL_INTERNAL	RAN Authentications – Internal Failure
38	RAN_AUTH_FAIL_STREAM_SELECTION_FAILED	RAN Authentications – Stream Selection Failures

Value	Count Group	SM COUNT DESCRIPTION
39	RAN_AUTH_FAIL_AT_CONFIG_RJCT_RCVD	RAN Authentication Failure – AT Configuration Reject Received
40	RAN_AUTH_FAIL_INVLD_AT_CFGRQ_PPP_EST_FLD	RAN Authentication Failure – Invalid AT Configuration Request PPP Establishment Failed
41	RAN_AUTH_FAIL_LCP_RLTD_PPP_EST_FAILED	RAN Authentication Configuration - ACK Related PPP Establishment Failures
42	RAN_AUTH_FAIL_CNFGR_NAK_PPP_EST_FAILED	RAN Authentication Configure- NAK Related PPP Establishment Failures
43	RAN_AUTH_FAIL_LCP_TERM_RCVD	RAN Authentication Failures – LCP Termination Received
44	RAN_AUTH_FAIL_NO_AT_CONFIG_RQST_RCVD	RAN Authentication Failures - No AT Configure Request Received
45	AT_INIT_CONN_ATTMPT_FAIL_NO_RES_AVLBL_SESS	AT-Initiated Connection Attempt Failures - No Resource Available –Session Setup Short
46	AT_INIT_CONN_ATTMPT_FAIL_RL_NOT_ACQ_SESS	AT-Initiated Connection Attempt Failures - Reverse Link Not Acquired - Session Setup Short
47	AT_INIT_CONN_ATTMPT_FAIL_NO_TCC_RCVD_SESS	AT-Initiated Connection Attempt Failures - No Traffic Channel Complete Received - Session Setup Short
48	AT_INIT_CONN_REQ_SESS	AT Initiated Connection Request - Session Setup Short
49	TCA_FOR_AT_INIT_CONN_REQ_SESS	AT Initiated Connection Request TCA Sent - Session Setup Short
50	AT_INIT_ESTABLISHED_CONN_SESS	AT Initiated Connection Request Established Connections - Session Setup Short
51	SESS_SETUP_REQ_POOR_RF_ALLOW	Session Setup Request Poor RF Allow Short
52	SESS_SETUP_REQ_POOR_RF_DENY	SessSU Req Poor RF Deny Short
53	HHOFF_ATTMPT_AN_DIRECT_UPPER_REQ	AN-Directed Hard Handoff Attempts Triggered by Upper Distance Threshold - Requesting Sector
54	HHOFF_ATTMPT_AN_DIRECT_PILOT_REQ	AN-Directed Hard Handoff Attempts Triggered by Pilot Strength Measurements – Requesting Sector

Value	Count Group	SM COUNT DESCRIPTION
55	HHOFF_FAIL_AN_DIRECT_ UPPER_REQ	Failed AN-Directed Hard Handoff Triggered by Upper Distance Threshold – Requesting Sector
56	HHOFF_FAIL_AN_DIRECT _PILOT_REQ	Failed AN-Directed Hard Handoff Triggered by Pilot Strength Measurements – Requesting Sector
57	HRPD_VOIP_1X_HO_REJECT	HRPD VoIP to 1X Circuit HO Rejection by 3G1X System
58	HRPD_VOIP_1X_HO_FAIL	VoIP to 1X Circuit A21 HHO Failures
59	CB_HHOFF_ATTMPT_REQ	Cross Band Hard Handoff Attempts - Requesting Sector
60	CB_HHOFF_CONN_CLOSE_REQ	Cross Band Hard Handoff Connection/ Session Close - Requesting Sector
61	CB_HHOFF_SUCC_REQ	Cross Band Hard Handoff Success - Requesting Sector
62	RAN_REAUTH_SUCCESSFUL_ ATTMPTS	RAN Re-Authentication Successful Attempts
63	RAN_REAUTH_FAILURE_ ATTMPTS	RAN Re-Authentication Failure Attempts
64	AT_INIT_CONN_ATMPT_REJ_ EHRPD_LIC_EXCEED	AT-Initiated Connection Attempt Rejections - eHRPD Connection License Exceeded
65	AN_INIT_CONN_ATMPT_REJ_ EHRPD_LIC_EXCEED	AN-Initiated Connection Attempt Rejections - eHRPD Connection License Exceeded
66	ESTABLISHED_CONN_ONE_ CARR_REVB	Rev B Connections Established with One Carrier
67	ESTABLISHED_CONN_TWO_ CARR_REVB	Rev B Connections Established with Two Carriers
68	ESTABLISHED_CONN_THREE_ CARR_REVB	Rev B Connections Established with Three Carriers
69	MC_TCA_FST_CARR_REVB	Rev B Traffic Channel Assignment for First Carrier
70	CONN_ATTMPT_FAIL_RL_NOT_ ACQ_REVB	Rev B Connection Attempt Failures - Reverse Link Not Acquired
71	CONN_ATTMPT_FAIL_OTHER_ PRETCA_REVB	Rev B Connection Attempt Failures - Other Reasons Pre TCA
72	CONN_ATTMPT_FAIL_OTHER_ POSTTCA_REVB	Rev B Connection Attempt Failures - Other Reasons Post TCA

Value	Count Group	SM COUNT DESCRIPTION
73	CONN_ATTMPT_FAIL_NO_TCC_RCVD_REVB	Rev B Connection Attempt Failures - No TCC Received
74	MC_TCA_TWO_CARR_REVB	Additional MC-TCA with Two Carriers
75	MC_TCA_THREE_CARR_REVB	Additional MC-TCA with Three Carriers
76	MC_TCA_FAIL_NO_TCC_REVB	MC-TCA Failures - Call released due to no TCC Received
77	MC_TCA_REDUC_RLACQ_FAIL_REVB	MC-TCA Carrier Reduction - Additional Carrier Reverse Link Acquisition Failure
78	CONN_SETUP_PERS_SWITCH_UNKNOWN_TO_REVB	Personality Switches During Connection Setup From Unknown to Rev B
79	CONN_SETUP_PERS_SWITCH_REL0_TO_REVB	Personality Switches During Connection Setup From Rel 0 to Rev B
80	CONN_SETUP_PERS_SWITCH_REVA_TO_REVB	Personality Switches During Connection Setup From Rev A to Rev B
81	CONN_SETUP_PERS_SWITCH_REVB_TO_REVA	Personality Switches During Connection Setup From Rev B to Rev
82	CONN_SETUP_PERS_SWITCH_REVB_TO_REL0	Personality Switches During Connection Setup From Rev B to Rel 0
83	CARR_DROPPED_RLL_REVB	RevB Carriers Dropped - Reverse Link Lost
84	RCCD_ONE_CARR_REVB	ReverseCDMAChannelDropped Received -- AT Dropped One Carrier
85	RCCD_TWO_CARR_REVB	ReverseCDMAChannelDropped Received — AT Dropped Two Carriers
86	CAR_COMPL_TWO_CARR_REVB	CarrierRequests Completed — Connection has Two Carriers
87	CAR_COMPL_THREE_CARR_REVB	CarrierRequests Completed - Connection has Three Carriers
88	CARR_ADD_ONE_RUM_PROC	Dynamic Carrier Addition During Rum Processing - One Carrier Added
89	CARR_ADD_TWO_RUM_PROC	Dynamic Carrier Addition During RUM Processing - Two Carriers Added
90	SHO_MC_CARR_REDUCTION_REQ	Soft/Softer Multi-Carrier Handoffs with Carriers Reduced -Requesting Sector
91	SHO_MC_CARR_UNCHANGED_REQ	Soft/Softer Multi-Carrier Handoffs with Carriers Unchanged -Requesting Sector

Value	Count Group	SM COUNT DESCRIPTION
92	AHO_PERS_SWTCH_REVB_TO_REL0	Number of Personality Switches During Active Connections from Rev B to Rel 0
93	AHO_PERS_SWTCH_REVB_TO_REVA	Number of Personality Switches During Active Connections from Rev B to Rev A
94	INT_SUBNET_IDL_TRFR_PRIOR_SES_BAD_REQ	Refer to Corresponding Service Measurement Definition.
95	ISBNT_IDL_TRFR_FAIL_PRIOR_SES_INVLD_SRC_AN_IP_ADR	Refer to Corresponding Service Measurement Definition.
96	ISBNT_IDL_TRFR_FAIL_PRIOR_SES_NO_RSP	Refer to Corresponding Service Measurement Definition.
97	ISBNT_IDL_TRFR_FAIL_PRIOR_SES_RJCT_MSG_RCVD	Refer to Corresponding Service Measurement Definition.
98	ISBNT_IDL_TRFR_FAIL_PRIOR_SES_UNREC_PERS	Refer to Corresponding Service Measurement Definition.
99	ISBNT_IDL_TRFR_FAIL_PRIOR_SES_OTHER_REASON	Refer to Corresponding Service Measurement Definition.
100	IVHHO_BLOCKED_NO_REJECT_SOURCE	Refer to Corresponding Service Measurement Definition.
102	AT_CONN_ATTEMPT_REDIRECTED	Connection Attempt was redirected to another EVDO carrier.
103	RAN_AUTH_DENY_BLOCKED_LIST	RAN Authentication - Access Denied Due to Blocked Domain List. See the corresponding service measurement definition.
104	CONN_REL_INTRFR_FEMTO	Connection Release˙C Interference from Femto Cell. See the corresponding service measurement definition.
105	ISBNT_IDL_TRFR_DENY_FEMTO	Inter-Subnet Idle Transfer Denial Due to Femto Cell for Color Code Method. See the corresponding service measurement definition.
106	ISBNT_IDL_TRFR_DENY_PRIOR_SES_FEMTO	Inter-Subnet Idle Transfer Denial Due to Femto Cell for Prior Session Method. See the corresponding service measurement definition.
107	NLB_1_LEG	Network Load Balance Events - 1 Leg Forced_Out_Of_Lock. See the corresponding service measurement definition.
108	NLB_2_LEG	Network Load Balance Events - 2 Legs Forced_Out_Of_Lock. See the corresponding service measurement definition.

Value	Count Group	SM COUNT DESCRIPTION
109	NLB_3_LEG	Network Load Balance Events - 3 or More Legs Forced_Out_Of_Lock. See the corresponding service measurement definition.

CFIM Field Requirement Location For Autoplex PCMD Data

Purpose

The table gives the mapping between the CFIM field and the PCMD field.

Here is the key:

- Italics: CFIM field name
- Lower case bold: NTP database table name

CFIM Field Name	PCMD field	PCMD description
Acc_chan	61	Access channel number
Announce_num	63	Announcement number
Answer_time	84	Call established time
Assign_carrier	26	Assigned Carrier
Avgnoise_rvrlink	129	Average RSSI-rise in the Reverse Link Carrier
Avgpwr_fwdlink	128	Average Power in the Forward Link Carrier
Backhaul_fac	79 80 81	Backhaul CDM Backhaul server number Backhaul number
Backhaul_rt_delay	124	Backhaul Round Trip Delay
Billdigits	7	Subscriber Number
Call_delivery	17	Call Delivery Type
Callid	2	Sequence Number
callstart_time	3	Call answer time
Carrier_band	28	assigned carrier band
Caus	39	CFC Qualifier
Caus2	40	Secondary CFC Qualifier
Ccc	60	CCC_CRC_URC
Ccu	12	Initial CCU
cdn	136	CDN Where the Call is Handled
Ce	13	Initial channel element number
Cell	10	Initial cell site number

CFIM Field Name	PCMD field	PCMD description
Celltgid	113	Final Packet Pipe Trunk Group Number
Celltgmem	114	Final Packet Pipe Trunk Group Member Number
Cell_start	142	Cell Based Call Start Timestamp
Cell_type	23	Cell type at start of call
Cic	Lookup in **owner**	-
Conn	49	Service connection complete flag
Cpdigits	7 if *d*=o	-
Cpfail_fdc1	120	CP Failure Reason 1
Cpfail_fdc2	121	CP Failure Reason 2
Cpfail_fdc3	122	CP Failure Reason 3
Ct	5	Call processing call type
D	“o” if 52 is zero “i” otherwise	-
Datacall_react	87	3G1X Data Call Reactivation
Dcs	20	PSTN DCS number
Dst_enabled	101	DST in effect
Dcs	20	Pstn dcs number
De	38 is key to a lookup	Call final class
Delay	41	CDMA round trip delay
Digits	7 if *d*=I 22 if *d*=o	Subscriber number Originated digits
Dst_enabled	101	DST in effect
Durat	4/1000	Call length
End_carrier	27	Ending carrier
End_datime	Timezone offset of *local_end*	-
Error_origin	Lookup into **acode2fdc**	-
Evrc_chgopt	115	EVRC-B to EVRC Service Option Change
Evrc_fwd	95	Initial Vocoder Forward Mode

CFIM Field Name	PCMD field	PCMD description
Evrc_rvrse	96	Initial Vocoder Reverse Mode
Fdc	Lookup in **acode2fdc** using field 39	CFC Qualifier
Final_backhaul_sm	116	Final Backhaul Server SM
Final_backhaul_psu	117	Final Backhaul Server PSU
Final_cdm_sig	118	Final for CDM Signaling Traffic
Final_cell_durat	141	Final Cell Total Time Duration
Final_mlg_sig	119	Final MLG for Signaling Traffic
Handoffs	21	Number of intra-DCS hand-offs
Handoff_rec	29	Call handed-in from another msc flag
Ho_time	130	Timestamp of the Last Completed Handoff
Iblm_fail	137	IBLM Redirection in MT
Ibyte	104	Transmitted RLP Bytes on F-FCH with RE-Transmission On
Iibtyte_reoff	110	Transmitted RLP Bytes on F-FCH with Re-transmission off
Ibyte_reoffsupp	111	Transmitted RLP Bytes on F-SCH with Re-transmission Off
Ibyte_resupp	108	Re-Transmitted RLP Bytes on F-SCH
Ibyte_retrans	107	Re-Transmitted RLP Bytes on F-SCH
Ict	19 if *d*=I	Pstn member number
Imsi	9	Imsi
Incall_time	102	INCALL Time
Itgid	18 if *d*=I	Pstn trunk number
Initbkhsm	131	Initial Backhaul Server SM

CFIM Field Name	PCMD field	PCMD description
Initbkhpsu	132	Initial Backhaul Server PSU
Initpgtime	103	Initial MSC Page Request Time
Init_cell_durat	140	Initial Cell Total Time
Jip	69	Jurisdiction Information parameter
Lac	78	Last Seen Local Area
Last_band	92	Ending Band Class
Last_callid	the callid value from the previously received record	
Last_ccc	82	Last CCC
Last_ccu	16	Last ccu
Last_ce	17	Last ce
Last_cell	14	Last cell
Last_cell_type	24	Cell type at end of call
Last_sector	15	Last sector
Last_sm	73	last SM
Last_tech	65	Ending technology type
Lnp	68	Wireless number portability flag
Local_end	3 & 4	Call answer time + call length
Local_start	3	Call answer time
Manfact	6	Serial Number
Rnc	86	RNC ID
Miles	Derived from *Delay* field	Call distance
Min	8	Mobile id number
Ms_type	64	Terminal information
Msc	98 97	ECP ID System ID
Multi_term	22	Multiple Termination Flag
Num_pages	42	Number of cdma pages

CFIM Field Name	PCMD field	PCMD description
Obyte	106	Transmitted RLP Bytes on RCH with Re-Transmission On
Obyte_reoff	112	Re-Transmitted RLP Bytes on RCH with Re-Transmission Off
Obyte_retrans	109	Re-Transmitted RLP Bytes on RCH
Ogt	19 if *d*=o	Pstn member number
Orig_msc	97	Switch ID
Otgid	18 if *d*=o	Pstn trunk group
Page_chan	62	Paging channel number
Page_tech1	74	Paging technique 1
Page_tech2	75	Paging technique 2
Page_tech3	76	Paging technique 3
Page_tech4	77	Paging technique 4
Pcf_id	93	PCF ID
Pcf_type	85	PCF Type
Pdsn	94	PDSN IP Address
Pptgid	43	Initial PP Trunk Group Number
Pptgmem	44	Initial PP Trunk Group Member Number
Pri_call_type	154	Priority Call Type
Pstn_tgtype	133	PSTN Trunk Unit Type
Pstn_tgn	134	PSTN Trunk DLTU, DNUS or OIU Number
Rad_fwd_config	45	Forward traffic channel radio configuration
Rad_rvrse_config	46	Reverse traffic channel radio configuration
Re	Lookup into **source**	-

CFIM Field Name	PCMD field	PCMD description
Reason	83 (also: the reason field is populated using the code2text table)	Inter-band Load Management overflow reason
Reason2	19	ISUP Cause Code
Related	The *related* field is derived from the combination of fields 9, 10 and 11	(Switch Identifier, ECP Identifier, and System Identifier)
Req_st	30	Requested service option
Roam_digs	18	Destination Digits
S	38 based	Call final state
Sctn	32	Speech handler trunk group
Sctn_dcs	34	Speech handler DCS number
Sctn_mem	33	Speech handler trunk group member
Sctn_sm	72	speech handler switching module
Sector	11	Initial sector
Seiz_carrier	25	Seizure carrier
Seizure_tech	36	Seizure technology type
Serno	6	Serial number
Sh_tg	135	Speech Handler Trunk PSU
Shared_mlg	123	Shared Ending MLG Flag
Silent_reorig	35	Silent re-origination flag
Sm	20	Pstn DCS number
Sm_cnt1	53	Service measurement count 1
Sm_cnt2	54	Service measurement count 2
Sm_cnt3	55	Service measurement count 3
Sm_cnt4	56	Service measurement count 4
Sm_cnt5	57	Service measurement count 5
Sm_cnt6	58	Service measurement count 6
Sm_cnt7	88	Num of SM Count
Sm_cnt8	89	Num of SM Count

CFIM Field Name	PCMD field	PCMD description
Sm_cnt9	90	Num of SM Count
Sm_cnt10	91	Num of SM Count
Sms_ct	50	Sms call type
Sms_msg_length	51	Sms message length
St	31	Allocated service option
Start_datime	Timezone offset of *local_start*	-
Tc	38	Call final state
Tcsi_timer	47	Traffic channel supervision interval timer
Tcsi_value	48	Traffic channel supervision interval timer value
Tech	37	Assigned technology type
Tgn	18	Pstn trunk group
Third_party_leg	66	Third party leg flag
Trb	40	Secondary cfc qualifier
Win	67	Wireless Intelligent Networking Call

PSMM Mapping for CFIM

Purpose

PCMD records can contain a section of data called Pilot Strength Measurement Messages (PSMM), which are comprised of data useful to understanding RF conditions in the network.

CFIM Field Name	Description
psmm_send_time	Time PSMM data was sent from cell (w/ 10ths of seconds)
psmm_cell	Identity of primary cell site
psmm_sector	Identity of the sector on the primary cell
psmm_delay	Round trip delay for the primary cell
psmm_ref1_timestamp_1	Time Reference PSMM message was collected
psmm_ref1_cell_1	Identity of reference cell site
psmm_ref1_sector_1	Identity of sector on the reference cell
psmm_ref1_carrier_1	Reference CDMA carrier number
psmm_ref1_num_pilots_1	Number of pilots for the reference set
psmm_ref1_pn_offset_1	Reference pilot pseudo noise (PN) offset
psmm_ref1_pilot_str_1	Reference pilot strength
psmm_ref1_keep_ind_1	Reference keep indicator
psmm_ref1_as_pre_1	Indicates whether reference sector is part of active set before handoff
psmm_ref1_as_post_1	Indicates whether reference sector is part of active set after handoff.
psmm_ref1_ho_comp_1	Handoff Complete Flag, first data set
psmm_nref1_cell_1	Identity of 1st non-reference cell site
psmm_nref1_sector_1	Identity of the sector on the 1st non-reference cell
psmm_nref1_pilot_str_1	1st non-reference pilot strength
psmm_nref1_keep_ind_1	1st non-reference keep indicator
psmm_nref1_pn_phase_1	1st non-reference phase of pilot PN sequence
psmm_nref1_as_pre_1	Indicates whether 1st non-reference sector is part of active set before handoff

CFIM Field Name	Description
psmm_nref1_as_post_1	Indicates whether 1st non-reference sector is part of active set after handoff
psmm_nref1_ho_comp_1	Handoff Complete Flag, first data set
psmm_nref2_cell_1	Identity of 2nd non-reference cell site
psmm_nref2_sector_1	Identity of the sector on the 2nd non-reference cell
psmm_nref2_pilot_str_1	2nd non-reference pilot strength
psmm_nref2_keep_ind_1	2nd non-reference keep indicator
psmm_nref2_pn_phase_1	2nd non-reference phase of pilot PN sequence
psmm_nref2_as_pre_1	Indicates whether 2nd non-reference sector is part of active set before handoff
psmm_nref2_as_post_1	Indicates whether 2nd non-reference sector is part of active set after handoff
psmm_nref2_ho_comp_1	Handoff Complete Flag, first data set
psmm_nref3_cell_1	Identity of 3rd non-reference cell site
psmm_nref3_sector_1	Identity of the sector on the 3rd non-reference cell
psmm_nref3_pilot_str_1	3rd non-reference pilot strength
psmm_nref3_keep_ind_1	3rd non-reference keep indicator
psmm_nref3_pn_phase_1	3rd non-reference phase of pilot PN sequence
psmm_nref3_as_pre_1	Indicates whether 3rd non-reference sector is part of active set before handoff
psmm_nref3_as_post_1	Indicates whether 3rd non-reference sector is part of active set after handoff
psmm_nref3_ho_comp_1	Handoff Complete Flag, first data set
psmm_nref4_cell_1	Identity of 4th non-reference cell site
psmm_nref4_sector_1	Identity of the sector on the 4th non-reference cell
psmm_nref4_pilot_str_1	4th non-reference pilot strength
psmm_nref4_keep_ind_1	4th non-reference keep indicator
psmm_nref4_pn_phase_1	4th non-reference phase of pilot PN sequence
psmm_nref4_as_pre_1	Indicates whether 4th non-reference sector is part of active set before handoff

CFIM Field Name	Description
psmm_nref4_as_post_1	Indicates whether 4th non-reference sector is part of active set after handoff
psmm_nref4_ho_comp_1	Handoff Complete Flag, first data set
psmm_nref5_cell_1	Identity of 5th non-reference cell site
psmm_nref5_sector_1	Identity of the sector on the 5th non-reference cell
psmm_nref5_pilot_str_1	5th non-reference pilot strength
psmm_nref5_keep_ind_1	5th non-reference keep indicator
psmm_nref5_pn_phase_1	5th non-reference phase of pilot PN sequence
psmm_nref5_as_pre_1	Indicates whether 5th non-reference sector is part of active set before handoff
psmm_nref5_as_post_1	Indicates whether 5th non-reference sector is part of active set after handoff
psmm_nref5_ho_comp_1	Handoff Complete Flag, first data set
psmm_ref1_timestamp_2	Time Reference PSMM message was collected
psmm_ref1_cell_2	Identity of reference cell site
psmm_ref1_sector_2	Identity of setor on the reference cell
psmm_ref1_carrier_2	Reference CDMA carrier number
psmm_ref1_num_pilots_2	Number of pilots for the reference set
psmm_ref1_pn_offset_2	Reference pilot pseudo noise (PN) offset
psmm_ref1_pilot_str_2	Reference pilot strength
psmm_ref1_keep_ind_2	Reference keep indicator
psmm_ref1_as_pre_2	Indicates whether reference sector is part of active set before handoff
psmm_ref1_as_post_2	Indicates whether reference sector is part of active set after handoff.
psmm_ref1_ho_comp_2	Handoff Complete Flag, second data set
psmm_nref1_cell_2	Identity of 1st non-reference cell site
psmm_nref1_sector_2	Identity of the sector on the 1st non-reference cell
psmm_nref1_pilot_str_2	1st non-reference pilot strength
psmm_nref1_keep_ind_2	1st non-reference keep indicator
psmm_nref1_pn_phase_2	1st non-reference phase of pilot PN sequence

CFIM Field Name	Description
psmm_nref1_as_pre_2	Indicates whether 1st non-reference sector is part of active set before handoff
psmm_nref1_as_post_2	Indicates whether 1st non-reference sector is part of active set after handoff
psmm_nref1_ho_comp_2	Handoff Complete Flag, second data set
psmm_nref2_cell_2	Identity of 2nd non-reference cell site
psmm_nref2_sector_2	Identity of the sector on the 2nd non-reference cell
psmm_nref2_pilot_str_2	2nd non-reference pilot strength
psmm_nref2_keep_ind_2	2nd non-reference keep indicator
psmm_nref2_pn_phase_2	2nd non-reference phase of pilot PN sequence
psmm_nref2_as_pre_2	Indicates whether 2nd non-reference sector is part of active set before handoff
psmm_nref2_as_post_2	Indicates whether 2nd non-reference sector is part of active set after handoff
psmm_nref2_ho_comp_2	Handoff Complete Flag, second data set
psmm_nref3_cell_2	Identity of 3rd non-reference cell site
psmm_nref3_sector_2	Identity of the sector on the 3rd non-reference cell
psmm_nref3_pilot_str_2	3rd non-reference pilot strength
psmm_nref3_keep_ind_2	3rd non-reference keep indicator
psmm_nref3_pn_phase_2	3rd non-reference phase of pilot PN sequence
psmm_nref3_as_pre_2	Indicates whether 3rd non-reference sector is part of active set before handoff
psmm_nref3_as_post_2	Indicates whether 3rd non-reference sector is part of active set after handoff
psmm_nref3_ho_comp_2	Handoff Complete Flag, second data set
psmm_nref4_cell_2	Identity of 4th non-reference cell site
psmm_nref4_sector_2	Identity of the sector on the 4th non-reference cell
psmm_nref4_pilot_str_2	4th non-reference pilot strength
psmm_nref4_keep_ind_2	4th non-reference keep indicator
psmm_nref4_pn_phase_2	4th non-reference phase of pilot PN sequence

CFIM Field Name	Description
psmm_nref4_as_pre_2	Indicates whether 4th non-reference sector is part of active set before handoff
psmm_nref4_as_post_2	Indicates whether 4th non-reference sector is part of active set after handoff
psmm_nref4_ho_comp_2	Handoff Complete Flag, second data set
psmm_nref5_cell_2	Identity of 5th non-reference cell site
psmm_nref5_sector_2	Identity of the sector on the 5th non-reference cell
psmm_nref5_pilot_str_2	5th non-reference pilot strength
psmm_nref5_keep_ind_2	5th non-reference keep indicator
psmm_nref5_pn_phase_2	5th non-reference phase of pilot PN sequence
psmm_nref5_as_pre_2	Indicates whether 5th non-reference sector is part of active set before handoff
psmm_nref5_as_post_2	Indicates whether 5th non-reference sector is part of active set after handoff
psmm_nref5_ho_comp_2	Handoff Complete Flag, second data set
psmm_agg_pilot_str_1	Field for the aggregate pilot strength of: psmm_ref1_pilot_str_1, psmm_nref1_pilot_str_1, psmm_nref2_pilot_str_1, psmm_nref3_pilot_str_1, psmm_nref4_pilot_str_1, and psmm_nref5_pilot_str_1
psmm_agg_pilot_str_2	Field for the aggregate pilot strength of: psmm_ref1_pilot_str_2, psmm_nref1_pilot_str_2, psmm_nref2_pilot_str_2, psmm_nref3_pilot_str_2, psmm_nref4_pilot_str_2, and psmm_nref5_pilot_str_2

DMS MTX CFIM Mapping

Purpose

The table below contains the mapping between the fields in the NTP CFIM data record and the fields in the message. The columns pertain to the LOG messages received from the DMS MTX switch.

Here is the key:

- Italics: CFIM field name
- ALL CAPITAL LETTERS: field name in the raw message
- Lower case bold: NTP database table name

CFIM Field Name	**cell**	**clfl**	**drop**	**cdma**	**c7up**	**trk**	**tcap**
acc_chan	-	-	Control Channel	-	-	-	-
acsstype (access type)	ACCESS	-	-	-	-	-	-
assigned_ carrier	CDMA	CDMA	RF Channel	CDMA	-	-	-
billdigits	MIN	MIN	MIN	MIN	-	-	-
callid (callid)	CALLID, TRID, or TRANS-ACTION ID	CALLID, TRID, or TRANS-ACTION ID	CALLID, TRID, or TRANS-ACTION ID	-	CALLID, TRID, or TRANS-ACTION ID	CALLID, TRID, or TRANS-ACTION ID	CALLID, TRID, or TRANS-ACTION ID
ce	-	-	Voice Channel	-	-	-	-
cell	CELL	CELL	CELL		-	-	-
chan_ type	MODE	MODE	MODE	MODE	-	-	-
cic (carrier id code)	-	-	-	-	-	CIC or CAR-RIER	-

CFIM Field Name	cell	clfl	drop	cdma	c7up	trk	tcap
cim (call irregularity message	Raw message	Raw message	Raw message	-	Raw message	Raw message	Raw message
cntlid	ICP or CSC (cell site controller)	ICP or CSC (cell site controller)	ICP or CSC (cell site controller)	ICP or CSC (cell site controller)	-	-	-
cpdigits (calling party digits)	ORIG DN, MIN, CALLING NUMBER, or MSID	ORIG DN, MIN, CALLING NUMBER, or MSID	ORIG DN, MIN, CALLING NUMBER, or MSID	ORIG DN, MIN, CALLING NUMBER, or MSID	Any number of fields	Any number of fields	Any number of fields
ct (call type)	CALLTYPE	CALLTYPE	CALLTYPE	CALLTYPE	-	-	-
d (call direction)	Lookup into **fdc**	Lookup into **fdc**	Lookup into **fdc**	Lookup into **fdc**	Lookup into **fdc**	Lookup into **fdc**	Lookup into **fdc**
date (date message was collected by NTP))	Date	Date	Date	-	Date	Date	Date
datime (date and time message was collected by NTP)	Date and time	Date and time	Date and time	-	Date and time	Date and time	Date and time

CFIM Field Name	cell	clfl	drop	cdma	c7up	trk	tcap
de (distant entity type)	Lookup into **cellroute** w/ CELL	Lookup into **cellroute** w/ CELL	Lookup into **cellroute** w/ CELL	Lookup into **cellroute** w/ CELL	Lookup into **dmsroute** w/ tgclli	Lookup into **dmsroute** w/ tgclli	Lookup into **dmsroute** w/ tgclli
detype (distant entity type)	Lookup into swarch using *de*	Lookup into swarch using *de*	Lookup into swarch using *de*	-	Lookup into swarch using *de*	Lookup into swarch using *de*	Lookup into swarch using *de*
digits (dialed digits)	TERM DN, CALLED NUMBER, MDN, or DIALED NO	TERM DN, CALLED NUMBER, MDN, or DIALED NO	TERM DN, CALLED NUMBER, MDN, or DIALED NO	-	Any number of fields	Any number of fields	Any number of fields
dpc (destination point code)	-	-	-	-	-	-	CALLED ADDR
fdc (failure designator code)	Lookup into **acode2fdc** w/ trouble code	Lookup into **acode2fdc** w/ trouble code	Lookup into **acode2fdc** w/ trouble code	Lookup into **acode2fdc** w/ trouble code	Lookup into **acode2fdc** w/ trouble code	Lookup into **acode2fdc** w/ trouble code	Lookup into **acode2fdc** w/ trouble code
ict (incoming trunk)	Value after the incoming trunk group CLLI	Value after the incoming trunk group CLLI	Value after the incoming trunk group CLLI	-	Any number of fields	Any number of fields	Any number of fields
imsi	IMSI	IMSI	IMSI	IMSI	-	-	-
itgid	Incoming trunk group CLLI	Incoming trunk group CLLI	Incoming trunk group CLLI	-	Incoming trunk group CLLI	Incoming trunk group CLLI	Incoming trunk group CLLI

CFIM Field Name	cell	clfl	drop	cdma	c7up	trk	tcap
last_cell	Value after following key-words: SECOND CELL NUMBER, CELL2, 2ND CELL NUMBER, 2NDCELL	Value after following key-words: SECOND CELL NUMBER, CELL2, 2ND CELL NUMBER, 2NDCELL	Value after following key-words: SECOND CELL NUMBER, CELL2, 2ND CELL NUMBER, 2NDCELL	Value after following key-words: SECOND CELL NUMBER, CELL2, 2ND CELL NUMBER, 2NDCELL	-	-	-
min	MIN	MIN	MIN	MIN	-	-	-
misc4	DEST	DEST	DEST	-	-	-	-
misc5	STATE, TSI, or CALL-STATE	STATE, TSI, or CALL-STATE	STATE, TSI, or CALL-STATE	-	-	-	-
msgtype (message type)	OPCODE, BAD PACK-AGE TYPE, COMPO-NENT TYPE, or OM	OPCODE, BAD PACK-AGE TYPE, COMPO-NENT TYPE, or OM	OPCODE, BAD PACK-AGE TYPE, COMPO-NENT TYPE, or OM	-	-	-	-
ogt (outgo-ing trunk)	Values after the outgoing trunk group CLLI	Values after the outgoing trunk group CLLI	Values after the outgoing trunk group CLLI	-	Any number of fields	Any number of fields	Any number of fields
otgid	Outgoing Trunk Group CLLI	Outgoing Trunk Group CLLI	Outgoing Trunk Group CLLI	-	Outgoing Trunk Group CLLI	Outgoing Trunk Group CLLI	Outgoing Trunk Group CLLI

CFIM Field Name	cell	clfl	drop	cdma	c7up	trk	tcap
ra (radio number)	-	-	RADIO	-	-	-	-
reason	Lookup into **acode2fdc** for acode field for fdc determination.	Lookup into **acode2fdc** for acode field for fdc determination.	Lookup into **acode2fdc** for acode field for fdc determination.	Lookup into **acode2fdc** for acode field for fdc determination.	-	-	-
reason2	Lookup into **acode2fdc** for acode field for fdc determination.	Lookup into **acode2fdc** for acode field for fdc determination.	Lookup into **acode2fdc** for acode field for fdc determination.	Lookup into **acode2fdc** for acode field for fdc determination.	-	-	-
related (realted entity)	Lookup into **cellroute** w/ 2nd cell	Lookup into **cellroute** w/ 2nd cell	Lookup into **cellroute** w/ 2nd cell	-	Lookup into **dmsroute**	Lookup into **dmsroute**	Lookup into **dmsroute**
re (reporting entity)	From link information	From link information	From link information	-	From link information	From link information	From link information
retype (reporting entity type)	Lookup into swarch using *re*	Lookup into swarch using *re*	Lookup into swarch using *re*	-	Lookup into swarch using *re*	Lookup into swarch using *re*	Lookup into swarch using *re*
s (status)	Lookup into **fdc**	Lookup into **fdc**	Lookup into **fdc**	Lookup into **fdc**	Lookup into **fdc**	Lookup into **fdc**	Lookup into **fdc**

CFIM Field Name	cell	clfl	drop	cdma	c7up	trk	tcap
sctn (service circuit trunk num)	CSC (cell site controller)	CSC	CSC	-	-	MFRCVR CKT RCVRMF	-
serno (serial number)	SERNO, SERIAL, or SERIAL NUMBER	SERNO, SERIAL, or SERIAL NUMBER	SERNO, SERIAL, or SERIAL NUMBER	SERNO, SERIAL, or SERIAL NUMBER	-	-	-
sig (signaling)	Lookup in **dmsroute**	Lookup in **dmsroute**	Lookup in **dmsroute**	-	Lookup in **dmsroute**	Lookup in **dmsroute**	Lookup in **dmsroute**
source (link to NTP)	Based on link information	Based on link information	Based on link information	-	Based on link information	Based on link information	Based on link information
st (service type)	Lookup into **gtspec** or **fdc**	Lookup into **gtspec** or **fdc**	Lookup into **gtspec** or **fdc**	-	Lookup into **gtspec** or**fdc**	Lookup into **gtspec** or **fdc**	Lookup into **gtspec** or **fdc**
tc (trouble category)	Lookup into **fdc** using *fdc*	Lookup into **fdc** using *fdc*	Lookup into **fdc** using *fdc*	-	Lookup into **fdc** using *fdc*	Lookup into **fdc** using *fdc*	Lookup into **fdc** using *fdc*
tech	GEN	GEN	GEN	GEN	-	-	-
tgn (trunk group)	Lookup into **dmsroute**	Lookup into **dmsroute**	Lookup into **dmsroute**	-	Lookup into **dmsroute**	Lookup into **dmsroute**	Lookup into **dmsroute**
tmdelta (time delta)	TIMEDELTA		-	-	-	-	-
trb (trouble code)	Log Name	Log Name	Log Name	-	Log Name	Log Name	Log Name

CFIM Field Name	cell	clfl	drop	cdma	c7up	trk	tcap
time (time message was collected by NTP)	Time	Time	Time	-	Time	Time	Time

Autoplex Message Mapping

Purpose

The table below contains the mapping between the fields in the NTP CFIM data record and the fields in the message. The columns pertain to the report and MDII messages received from the Autoplex switch. In general, the value in the NTP CFIM table is the value after the key word listed in the table below.

Here is the key:

- Italics: CFIM field name
- ALL CAPITAL LETTERS: field name in the raw Autoplex message
- Lower case bold: NTP database table name

REPT and MDII Messages

NTP CFIM Field Name	AUTH FAIL	CELL CP FAIL	DCS CP FAIL	GEN SYSTEM CP FAIL	SCP DB FAIL	DCS FAIL	5E MDII
acc_chan (access channel number)	-	CHAN	-	CHAN	-	-	-
act (number of active trunks)	-	-	-	-	-	-	Based on OOS, SZ, TKGOOS, TGKMOOS, and/or TGSIZE
allow_tech (allowed technology)	-	ALW or ASFN for multi-technologies	-	ALW or ASFN for multi-technologies	-	-	-
ant (antenna)	ANT	ANT	-	ANT or SECTOR	-	-	-
Assign_carrier (assigned carrier)	-	CARRIER	-	CARRIER	-	-	-

NTP CFIM Field Name	AUTH FAIL	CELL CP FAIL	DCS CP FAIL	GEN SYSTEM CP FAIL	SCP DB FAIL	DCS FAIL	5E MDII
Bachaul_fac (back-haul facility)	-	BHS	-	-	-	-	-
billdigits (billing digits)	IMSI or cpdigits/ digits	MIN or last 10 digits of IMSI or cpdigits/ digits	-	MIN or last 10 digits of IMSI or cpdigits/ digits	-	-	-
Callid	-	ECID or CPCAL-LID	-	-	-	-	-
Caus	-	-	-	-	TCAP REJECT MES-SAGE	-	-
Caus2	-	-	-	-	2nd line after TCAP REJECT MES-SAGE	-	-
ccu (cdma channel unit number)	-	CCU	-	CCU	-	-	-
Cdn	-	CDN	-	-	-	-	-
ce (channel element number)	-	CE	-	CE	-	-	-
Cell	-	CELL or IMCELL	-	CELL or IMCELL	-	-	-
Celltgid	-	PP	-	-	-	-	-

NTP CFIM Field Name	AUTH FAIL	CELL CP FAIL	DCS CP FAIL	GEN SYSTEM CP FAIL	SCP DB FAIL	DCS FAIL	5E MDII
Celltype	-	Lookup in celltype table with cntlid & cpfail	-	Lookup in celltype table with cntlid & cpfail	-	-	-
cic (carrier id code)	-	-	-	-	-	Value below Inter-Exchange Carier RESULT label	ID
cim (call irregular-ity message)	Raw message	Raw message	Raw message	Raw message	Raw message	Raw message	Raw message
cntlid	-	CDM, MICRO, BBU or CCC label	-	CDM, MICRO, BBU or CCC label	-	-	-
conn	-	ANSWERED (y) OR UNAN-SWERED (n)	-	ANSWERED (y) OR UNAN-SWERED (n)	-	-	-
cpdigits (calling party digits)	If DN Is present, then DN else MIN	If CP FAILURE!= termination, then DN, else MIN	-	If CP FAILURE!= termination, then DN, else MIN	-	-	CALL-ING -NO

NTP CFIM Field Name	AUTH FAIL	CELL CP FAIL	DCS CP FAIL	GEN SYSTEM CP FAIL	SCP DB FAIL	DCS FAIL	5E MDII
ct (call type)	Lookup into **ctcode2ct** w/ ACCESS TYPE	Lookup into **ctcode2ct** w/ ANSWERED or UNAN-SWERED	-	Lookup into **ctcode2ct** w/ ANSWERED or UNAN-SWERED	-	-	-
d (call direc-tion)	Lookup into **fdc**	Lookup into **fdc**	Lookup into **fdc**	Lookup into **fdc**	Lookup into **fdc**	Lookup into **fdc**	If IGT exists, then "i", else if OGT exists, then "o"
date (date message was collected by NTP)	Date	Date	Date	Date	Date	Date	Date
datime (date and time message was collected by NTP)	Date and time	Date and time	Date and time	Date and time	Date and time	Date and time	Date and time
dcs	-	DCS	DCS	DCS		DCS	
de (distant entity)	Lookup into **cellroute** w/ SERV-ING CELL	Lookup into **cellroute** w/ CELL	-	Lookup into **cellroute** w/ CELL	Lookup into **gtspec** w/ DN	Lookup into **route5e** w/ TRKGRP	Lookup into **route5e** w/ TKGMN or TRK-GRP

NTP CFIM Field Name	AUTH FAIL	CELL CP FAIL	DCS CP FAIL	GEN SYSTEM CP FAIL	SCP DB FAIL	DCS FAIL	5E MDII
detype (distant entity type)	Lookup into swarch using *de*	Lookup into swarch using *de*	-	Lookup into swarch using *de*	Lookup into swarch using *de*	Lookup into swarch using *de*	Lookup into swarch using *de*
digits (dialed digits)	DIALED DIGITS	If TERMI-NATION then DN else MIN	-	If TERMI-NATION then DN else MIN	CALLED	-	CALLED -NO or ADDR-DIG
dl (data loss)	-	-	-	-	-	-	If DIS-CARD exists, set to "y"
dpc (destina-tion point code)	VLR PC	-	-	-	-	-	DPC
etime (event time)	TIME	-	-	-	TIME	-	TIME
fdc (failure designa-tor code)	Lookup into **acode2fdc** w/ FAIL URE TYPE	Lookup into **acode2fdc** using the line following "REPT-:CELL..."	Lookup into **acode2fdc** w/ DCS CP FAIL-URE	Lookup into **acode2fdc** using the line following "REPT-:GEN-ERAL..."	Lookup into **acode2fdc** using "TRANS ACTION ID"	Lookup into **acode2fdc** w/ REASON	MDII
ict (incom-ing trunk)	-	-	-	TM	-	-	TKGMN (if OGT not present) or MEMBER (if ICT present)

NTP CFIM Field Name	AUTH FAIL	CELL CP FAIL	DCS CP FAIL	GEN SYSTEM CP FAIL	SCP DB FAIL	DCS FAIL	5E MDII
imsi (intl mobile station id)	IMSI	IMSI	-	IMSI	-	-	-
lnp (local number portability)	-	-	-	-	-	-	LRN
lrn (location routing number)	-	-	-	-	-	-	If "LNP= DONE" then "y" else "n"
lrne (network element for call)	-	-	-	-	-	-	Only for LNP
manfact	Lookup using SNX in manufacturer tbl	Lookup using SNX in manufacturer tbl	-	Lookup using SNX in manufacturer tbl	-	-	-
Min	-	MIN	-	MIN	-	-	-
misc1	-	1st 25 char of acode string	-	-	acode	TYPE	-
misc2	-	FAILURE LOCATION	-	FAILURE LOCATION	-	-	-
misc3	FAILURE DATA	-	-	-	-	-	-

NTP CFIM Field Name	AUTH FAIL	CELL CP FAIL	DCS CP FAIL	GEN SYSTEM CP FAIL	SCP DB FAIL	DCS FAIL	5E MDII
misc4	The line following FAIL-URE DATA	-	-	-	-	-	-
mlg	-	MLG	-	-	-	-	-
msc	-	ECP ID or FS_ECP and SYS ID	-	FS_ECP and SYS ID	-	-	-
Msgtype	-	ASSERT or ASSERT CODE	-	-	-	-	-
ogt (origina-tion point code)	-	TM	-	TM	-	MEMBER	TKGMN (if ICT not present) or MEMBER (if OGT present)
opc (origina-tion point code)	-	-	-	-	-	-	OPC
psu	-	PSU	-	-	-	-	
r (related direc-tion)	-	RA	-	RA	-	-	-
ra (radio number)	-	RA	-	RA	-	-	-

NTP CFIM Field Name	AUTH FAIL	CELL CP FAIL	DCS CP FAIL	GEN SYSTEM CP FAIL	SCP DB FAIL	DCS FAIL	5E MDII
Reason	-	1st 60 char after acode string	-	1st 60 char after acode string	-	REASON	-
Reason2	-	2nd 60 char after acode string	-	-	-	-	-
related (related entity)	-	Lookup into **cellroute** w/ DCS	-	Lookup into **cellroute** w/ DCS	-	-	Only for lnp calls
re (report-ing entity)	From link info	From link info	From link info	From link info	From link info	From link info	From link info
retype (report-ing entity type)	Lookup into swarch using *re*	Lookup into swarch using *re*	Lookup into swarch using *re*	Lookup into swarch using *re*	Lookup into swarch using *re*	Lookup into swarch using *re*	Lookup into swarch using *re*
rnc	-	RNC	-	-	-	-	-
s (status)	'n' if ALLO -WED = yes, otherwise 'y'	Lookup into **fdc**	Lookup into **fdc**	Lookup into **fdc**	Lookup into **fdc**	Lookup into **fdc**	If TEST exists, then 'n', else Lookup into **fdc**
Scm	-	SCM	-	SCM	-	-	-
sctn (service circuit trunk num)	-	TG	-	-	-	-	UTD, UTG, RVPT, LDSU, LDSU2, TDEC, TGEN, or TXCVR

NTP CFIM Field Name	AUTH FAIL	CELL CP FAIL	DCS CP FAIL	GEN SYSTEM CP FAIL	SCP DB FAIL	DCS FAIL	5E MDII
Sctn_dcs	-	DCS	-	-	-	-	-
Sctn_ mem	-	TM	-	-	-	-	-
All fields prefixed with “sec1” are populated with data from the 1st line of the list of secondary cells							
Sec1_ccu	-	CCU	-	CCU	-	-	-
Sec1_ce	-	CE	-	CE	-	-	-
Sec1_cell	-	CELL	-	CELL	-	-	-
Sec1_cell_ type	-	Lookup in celltype tbl with sec1_ cntlid	-	Lookup in celltype tbl with sec1_ cntlid	-	-	-
Sec1_ celltgid	-	PP	-	PP	-	-	-
Sec1_ cntlid	-	CDM, MICRO, BBU, CCC	-	CDM, MICRO, BBU, CCC	-	-	-
Sec1_ msc	-	ECP ID and SYS ID	-	ECP ID and SYS ID	-	-	-
Sec1_ sector	-	SECTOR	-	SECTOR	-	-	-
All fields prefixed with “sec2” are populated with data from the 2nd line of the list of secondary cells							
Sec2_ccu	-	CCU	-	CCU	-	-	-
Sec2_ce	-	CE	-	CE	-	-	-
Sec2_cell	-	CELL	-	CELL	-	-	-

NTP CFIM Field Name	AUTH FAIL	CELL CP FAIL	DCS CP FAIL	GEN SYSTEM CP FAIL	SCP DB FAIL	DCS FAIL	5E MDII
Sec2_cell_type	-	Lookup in celltype tbl with sec1_ cntlid	-	Lookup in celltype tbl with sec1_ cntlid	-	-	-
Sec2_ celltgid	-	PP	-	PP	-	-	-
Sec2_ cntlid	-	CDM, MICRO, BBU, CCC	-	CDM, MICRO, BBU, CCC	-	-	-
Sec2_ msc	-	ECP ID and SYS ID	-	ECP ID and SYS ID	-	-	-
Sec2_ sector	-	SECTOR	-	SECTOR	-	-	-
All fields prefixed with “sec3” are populated with data from the 3rd line of the list of secondary cells							
Sec3_ccu	-	CCU	-	CCU	-	-	-
Sec3_ce	-	CE	-	CE	-	-	-
Sec3_cell	-	CELL	-	CELL	-	-	-
Sec3_cell_type	-	Lookup in celltype tbl with sec1_ cntlid	-	Lookup in celltype tbl with sec1_ cntlid	-	-	-
Sec3_ celltgid	-	PP	-	PP	-	-	-
Sec3_ cntlid	-	CDM, MICRO, BBU, CCC	-	CDM, MICRO, BBU, CCC	-	-	-

NTP CFIM Field Name	AUTH FAIL	CELL CP FAIL	DCS CP FAIL	GEN SYSTEM CP FAIL	SCP DB FAIL	DCS FAIL	5E MDII
Sec3_msc	-	ECP ID and SYS ID	-	ECP ID and SYS ID	-	-	-
Sec3_sector	-	SECTOR	-	SECTOR	-	-	-
All fields prefixed with “sec4” are populated with data from the 4th line of the list of secondary cells							
Sec4_ccu	-	CCU	-	CCU	-	-	-
Sec4_ce	-	CE	-	CE	-	-	-
Sec4_cell	-	CELL	-	CELL	-	-	-
Sec4_cell_type	-	Lookup in celltype tbl with sec1_cntlid	-	Lookup in celltype tbl with sec1_cntlid	-	-	-
Sec4_celltgid	-	PP	-	PP	-	-	-
Sec4_cntlid	-	CDM, MICRO, BBU, CCC	-	CDM, MICRO, BBU, CCC	-	-	-
Sec4_msc	-	ECP ID and SYS ID	-	ECP ID and SYS ID	-	-	-
Sec4_sector	-	SECTOR	-	SECTOR	-	-	-
All fields prefixed with “sec5” are populated with data from the 5th line of the list of secondary cells							
Sec5_ccu	-	CCU	-	CCU	-	-	-
Sec5_ce	-	CE	-	CE	-	-	-
Sec5_cell	-	CELL	-	CELL	-	-	-

NTP CFIM Field Name	AUTH FAIL	CELL CP FAIL	DCS CP FAIL	GEN SYSTEM CP FAIL	SCP DB FAIL	DCS FAIL	5E MDII
Sec5_cell_type	-	Lookup in celltype tbl with sec1_cntlid	-	Lookup in celltype tbl with sec1_cntlid	-	-	-
Sec5_celltgid	-	PP	-	PP	-	-	-
Sec5_cntlid	-	CDM, MICRO, BBU, CCC	-	CDM, MICRO, BBU, CCC	-	-	-
Sec5_msc	-	ECP ID and SYS ID	-	ECP ID and SYS ID	-	-	-
Sec5_sector	-	SECTOR	-	SECTOR	-	-	-
Sector	-	ANT	-	ANT or SECTOR	-	-	-
serno (serial number)	SN	SN X	-	SN X	-	-	-
sig (signal-ing)	-	-	-	-	-	-	SIG-TYPE
sg (server group)	SG	SG	-	SG	-	-	-
sm		SM	-	-	-	DATA	-
source (link to NTP	Based on link info	Based on link info	Based on link info	Based on link info	Based on link info	Based on link info	Based on link info
st (service type)	Lookup into **gtspec** or **fdc**	Lookup into **gtspec** or **fdc**	-	Lookup into **gtspec** or **fdc**	Lookup into **gtspec** or **fdc**	Lookup into **gtspec** or **fdc**	Lookup into **gtspec** or **fdc**

NTP CFIM Field Name	AUTH FAIL	CELL CP FAIL	DCS CP FAIL	GEN SYSTEM CP FAIL	SCP DB FAIL	DCS FAIL	5E MDII
trb	string authfail	string cpfail	string dcscpfail	string gensys-fail	String scpbfail	String dcsfail	
tc (trouble category)	Lookup into **fdc** using *fdc*	Lookup into **fdc** using *fdc*	Lookup into **fdc** using *fdc*	Lookup into **fdc** using *fdc*	Lookup into **fdc** using *fdc*	Lookup into **fdc** using *fdc*	Lookup into **fdc** using *fdc*
Tech	-	ASSGN		-		-	
tgn (trunk group)	-	TG	-	TG	-	TRKGRP	TKGMN or TRK-GRP
time (time message was collected by NTP)	Time	Time	Time	Time	Time	Time	Time
tnsc	-	-	-	-	-	-	TNSC
vrg (voice radio group)/	-	VRG	-	VRG	-	-	-

HEH MESSAGES

If the HEH Feature is enabled, the following will be present:

NTP CFIM Field Name	HEH
ampshelf	Value after TXAMPSHELF label
ant_atten	Value after IA VARIABLE ATTENUATOR label
ant_cal_loss	Value after IA CALIBRATION LOSS label
ant_fwd_mode	Value after IA FORWARD MODE label
ant_rev_mode	Value after IA REVERSE MODE label

assign_carrier	Value after CARRIER label; NULL for 924 format
backhaul_fac	Value after BHS; NULL for 925 format
carrier_band	Value g’
ccu	Value after CCU Label
ce	Value after CE Label
cell	CELL
cell_type	Lookup in celltype table with cntlid & cpfail
cntlid	CDM, MICRO or BBU
dcs	Value after DCS Label; NULL for 925 format
de	Lookup into cellroute using re and cell
ds1	Value after DS1 label ;NULL for 925 format
ds1_status	Text after the DS1 value
fdc	Acode2fdc look up using “ERROR TYPE” in format 924 or “FAILURE:” in format 925
Misc1	acode
misc3	SUPPRESSED MSGS
mlg	Value after MLG label ;NULL for 925 format.
msgtype	Value after “LAST ASSERT RECEIVED WAS:”, NULL for 925 format.
msgtype2	the assert number following the LAST ASSERT RECEIVED WAS: label
page_tech1	value immediately prior to HEH label (a’ field)
port	Vaue after TXPORT label
psu	Value after PSU label ;NULL for 925 format.
ra	Value after first CBR
ra2	Value immediately following the second CBR label
ra_path_1	first set of forward and/or reverse IA modes, TXPORT 1 or RXPORT 1 label
ra_path_2	second set of forward and/or reverse IA modes, TXPORT 1 or RXPORT 1 label
reason	Values in the f*** and (s or b’)**** ;NULL for 925 format.
rnc	Value after RNC label; NULL for 925 format.

s	Lookup into **fdc**
sector	Value after SECTOR label; NULL for 924 format.
sm	Value after SM label; NULL for 925 format.
st	Lookup into **gtspec** or **fdc**
tech	String CDMA
trb	String HEH
uname	Value c
unumber	Value after unumber
xuname	??
xunumber	??

EvDO PCMD Mapping for EVDO

Purpose

EvDO (Evolution – Data Optimized) is a wireless broadband technology used with CDMA technology. Table below describes fields for EvDO PCMD (Per Call Measurement Data) records obtained from the OMP in a Lucent EvDO network.

The EvDO PCMD record includes the following:

- PCMD (Per Call Measurement Data call record).
- RUM (Route Update Message indicating RF measurements for the call).

These records provides a view of connection establishment session failures, with a complete set of Call Final Classes and Call Final Class Qualifiers that is unique to PCMD. EvDO RUM records also provides a view of air-side problems affecting QOS which can be used by RF engineers in troubleshooting problems and understanding coverage.

Field	Description
A10_LINK_TIME	The a10_link_time field contains the timestamp indicating when the RNC established the bearer path to the PDSN for a connection.
A12_AUTH_TIME	The a12_auth_time field contains the timestamp indicating when the RNC made an authentication request to the Authentication server over the A12 interface.
ACC_CHAN	The acc_chan field contains the access channel number used to setup a call.
ACC_CHAN_2	Assigned Channel Number - Carrier 2
ACC_CHAN_3	Assigned Channel Number - Carrier 3
ANSWER_DATIME	Timestamp of call answer.
AP	The ap field identifies the application processor in the RNC that generated this message.
AP_IPADDR	The ap_ipaddr field contains the IP address of the Application Processor that is controlling the cell when the failure occurs.
AP_NUM	The identifier for the Application Processor (AP) containing the final controlling Overhead Manager (OHM) for the connection.
ASS_CELL_SER_NODE_ID	Assigned Cell's Service Node ID – For Connection or Personality Switch event, this field contains the Service Node ID of the assigned cell.
ASSIGN_CELL	The assign_cell field contains the assigned cell site ID for the connection in EvDO PCMD records.

Field	Description
ASSIGN_SECTOR	The assign_sector field contains the assigned sector ID for the connection in EvDO PCMD records.
AT_TYPE	The at_type field contains the Access Terminal (PC, PDA, Mobile handset. etc.) type.
CALLID	The callid field contains the call handle.
CARRIER_BAND	The carrier_band field contains the assigned carrier (cic) band. For REPT EVDO RNC CP FAIL messages, the carrier_band field contains the Band Class Identifier for the EvDO connection. For EvDO PCMD records, the carrier_band field contains the assigned band classes of the connection.
CAUS	The caus field contains the cause code associated with the failure as recorded in the Diagnostic or Result field.
CAUS2	The cause2 field contains the secondary cause code.
CELL	The cell field contains the initial cell site identifier.
CIM	The CIM field contains additional data from the original call information message, including some that has not been saved/converted into this CFIM record.
COLCODE	The colcode field contains the digital color code number used on the connection.
CONFIG_END	The config_end field contains the timestamp indicating the end of configuration negotiation.
CONFIG_ERROR	The config_error field contains the error code resulting from a failure in configuration negotiation.
CONFIG_START	The config_start field contains the timestamp indicating the start of configuration negotiation.
CONN	The conn field indicates whether the service connection was completed.
CONN_TYPE	The conn_type is the Connection type in the EvDO PCMD record.
CPCUSTTYPE	The cpcusttype field contains the calling party customer type as derived by the digits standardization feature. For EvDO PCMD records, the cpcusttype field contains the name of the subscriber as derived from the IMSI.
CPDIGITS	The calling party digits (cpdigits) field contains the digits of the calling party.
CPFAIL_FDC1	The cpfail_fdc1 is the Session or Connection CPFail Value (field 14) in the EvDO PCMD record.

Field	Description
CT	The ct field contains the call type associated with the structure code (found in the billtype field).
D	The call direction (d) field indicates the direction of the call involved in the irregularity, at the time it was detected. For EvDO PCMD records, a direction of (o) indicates the AT initiated the connection. A direction if (i) indicates the AN initiated the connection. A direction of (-) indicates a fast connection.
DATIME	The date field represents the date on which the system received the CIM.
DE	The date and time (datime) field combines the date and time field values together.
DETYPE	The distant entity (de) is the entity that the reporting office was attempting to communicate with when the call irregularity occurred.
DIGITS	The digit field contains the called number before translations.
DS	The distant entity home STP (ds) field contains the home STP pair of the distant entity.
DURAT	The durat field is the billable length of the call or session in seconds.
END_DATIME	The end_datime field contains the time when billing on the call or session was terminated, in datetime format (down to the second). For phone calls, this corresponds to call release.
FDC	The fdc field contains the reason for termination. This value must have been a fdc entry in the fdc table.

Field	Description
FL_ACT_DUR	The FL User Activity Duration field reports the length of time, in milliseconds, between the first packet of user data leaving the RNC and the last packet leaving the RNC for the connection. This field is a measure of the amount of time it took for the RNC to deliver user data on the forward link. It is not a measure of RNC performance because this value does not indicate how busy the RNC was or provide any data on what might have prevented the RNC from sending the connection's packets forward to the BTS. There are many elements, not just the RNC, that can contribute to transmission delay that are not captured in this field: the BTS, the air interface, or the backhaul itself. Therefore, it is not recommended to sum or average this value across connections as the value would be misleading. Post-processing tools can divide FL RLP Bytes by this field to estimate the FL throughput in bytes per millisecond on each connection where FL RLP Bytes is field 45.
FLOW_DIRECTION	The flow direction indicates the direction of the flow for an EvDO data connection. This corresponds to the last flow of the connection.
FLOW_DURAT	The Flow Event Duration field indicates the Flow Event Duration as the difference between Flow Established time and the end of the flow. For signaling flows, this field is blank because the duration is not known when the connection is terminated; the signaling flow remains up beyond the end of this connection (and this record).
FLOW_FC	The Flow Final Class field contains values to convey failure or success of the flow allocation and establishment. For signaling flows, this field is blank because there is no data on the conditions which caused a signaling flow to terminate; the signaling flow remains up beyond the end of this connection (and this record).
FLOW_FCQ	The Flow FC Qualifier field provides data conveying the reason for the disposition of the flow establishment request. For signaling flows, this field is blank because there is no data available indicating the final class qualifier of the flow; the signaling flow remains up beyond the end of this connection (and this record).
FLOW_FCQ2	The flow_fcq2 field indicates the final class secondary qualifier of the data flow for an EvDO data connection. This corresponds to the last flow of the connection.

Field	Description
FLOW_PROF_ID	This field indicates the Reservation Type Requested (Flow Profile ID) for the Flow. These Profile ID values are provisioned by the operator.
FLOW_REQ_CHANTYPE	The flow reservation on-request channel type indicates requested channel type of a flow for an EvDO data connection. This corresponds to the last flow of the connection.
FLOW_RES_DENIED	The flow reservation request denied flag indicates whether the flow reservation request was denied for an EvDO data connection. This corresponds to the last flow of the connection.
FLOW_RES_LABEL	The flow reservation label is an identifier of the flow reservation for an EvDO data connection. This corresponds to the last flow of the connection.
FLOW_RES_REQ	The flow reservation request time indicates the time that the flow reservation request was received by the Application Processor for an EvDO data connection. This corresponds to the last flow of the connection.
FLOW_START	The flow_start field indicates the time that the data flow began for an EvDO data connection. This corresponds to the last flow of the connection.
GAP_FOUND	The gap_found field contains a flag indicating whether a gap was found in the callid values for the current record and the last record.
HOME_IU_PRI	The Inter-user priority this subscriber has in the Home Jurisdiction area. This is used for possibility limiting bandwidth for roaming subscribers.
IBYTE	The ibyte field contains the byte count for the session from the egress to ingress side.
IBYTE_RETRANS	The ibyte_retrans field contains the number of inbound (downlink) bytes that were retransmitted during the connection.
ICT	The ict field contains the incoming trunk group member for the call.
IMSI	The imsi field contains the International Mobile Station Identity of the handset used for the call.
INCALL_TIME	The incall time field captures the time in seconds since midnight that the CDM receives the MG_INCALL message from the DSC. This is only applicable for call terminations.

Field	Description
INIT_AP	The IP address of the Initial Application Processor (AP) containing the Overhead Manager (OHM) for this connection. This may or may not be the final controlling Overhead Manager for the connection.
INIT_AP_NUM	The identifier for the Initial Application Processor (AP) containing the controlling Overhead Manager (OHM) for the connection. This may or may not be the final controlling Overhead Manager for the connection.
INIT_OHM	The init_ohm field indicates the initial Overhead Manager before transfer of session balance to a new Applications Processor and a new Overhead Manager.
ITGID	The itgid field contains the incoming trunk group for the call.
JIP	The jip field will provide the jurisdiction information parameter for the call. This parameter indicates the geographic origination of the call. For EvDO PCMD records, the jip field contains the Home Jurisdiction ID for the subscriber.
KPE_EVENT_CODE_1	Code for first Key Protocol Events
KPE_EVENT_TIME_1	Timestamp for first Key Protocol Events
KPE_EVENT_DATA_1	Data area for first Key Protocol Events
KPE_EVENT_CODE_2	Code for second Key Protocol Events
KPE_EVENT_TIME_2	Timestamp for second Key Protocol Events
KPE_EVENT_DATA_2	Data area for second Key Protocol Events
KPE_EVENT_CODE_3	Code for third Key Protocol Events
KPE_EVENT_TIME_3	Timestamp for third Key Protocol Events
KPE_EVENT_DATA_3	Data area for third Key Protocol Events
KPE_EVENT_CODE_4	Code for fourth Key Protocol Events
KPE_EVENT_TIME_4	Timestamp for fourth Key Protocol Events
KPE_EVENT_DATA_4	Data area for fourth Key Protocol Events
KPE_EVENT_CODE_5	Code for fifth Key Protocol Events
KPE_EVENT_TIME_5	Timestamp for fifth Key Protocol Events
KPE_EVENT_DATA_5	Data area for fifth Key Protocol Events
KPE_EVENT_CODE_6	Code for sixth Key Protocol Events
KPE_EVENT_TIME_6	Timestamp for sixth Key Protocol Events
KPE_EVENT_DATA_6	Data area for sixth Key Protocol Events
KPE_EVENT_CODE_7	Code for Key Protocol Events

Field	Description
KPE_EVENT_TIME_7	Timestamp for Key Protocol Events
KPE_EVENT_DATA_7	Data area for Key Protocol Events
KPE_EVENT_CODE_8	Code for Key Protocol Events
KPE_EVENT_TIME_8	Timestamp for Key Protocol Events
KPE_EVENT_DATA_8	Data area for Key Protocol Events
KPE_EVENT_CODE_9	Code for Key Protocol Events
KPE_EVENT_TIME_9	Timestamp for Key Protocol Events
KPE_EVENT_DATA_9	Data area for Key Protocol Events
KPE_EVENT_CODE_10	Code for Key Protocol Events
KPE_EVENT_TIME_10	Timestamp for Key Protocol Events
KPE_EVENT_DATA_10	Data area for Key Protocol Events
KPE_EVENT_CODE_11	Code for Key Protocol Events
KPE_EVENT_TIME_11	Timestamp for Key Protocol Events
KPE_EVENT_DATA_11	Data area for Key Protocol Events
KPE_EVENT_CODE_12	Code for Key Protocol Events
KPE_EVENT_TIME_12	Timestamp for Key Protocol Events
KPE_EVENT_DATA_12	Data area for Key Protocol Events
KPE_EVENT_CODE_13	Code for Key Protocol Events
KPE_EVENT_TIME_13	Timestamp for Key Protocol Events
KPE_EVENT_DATA_13	Data area for Key Protocol Events
KPE_EVENT_CODE_14	Code for Key Protocol Events
KPE_EVENT_TIME_14	Timestamp for Key Protocol Events
KPE_EVENT_DATA_14	Data area for Key Protocol Events
LAST_BAND	The last_band field contains the carrier band class at the end of the call. For PCMD records, the last_band field contains the ending band class for the call.
LAST_CALLID	The last_callid field will provide the last received call identifier.
LAST_CELL	The last_cell field contains the last cell site number.
LAST_CHAN	The last_chan field contains the channel number at the end of the call.
LAST_CHAN_2	Ending Channel Number - Carrier 2
LAST_CHAN_3	Ending Channel Number - Carrier 3

Field	Description
LAST_PG_AREA	The last_pg_area field contains the last attempted paging area for the EvDO PCMD connection.
LAST_PG_CELL	The last_pg_cell field contains the last-seen cell used for paging for the EvDO connection.
LAST_PG_GRPMEM	The last_pg_grpmem field contains the last-seen group member used for paging for the EvDO connection.
LAST_PG_SECTOR	The last_pg_sector field contains the last-seen sector used for paging for the EvDO connection.
LAST_SECTOR	The last_sector is the last sector number.
LOCAL_END	The local_end field contains the end of call time stamp (used for end_datime) using the local time of the re (i.e. the original end date and time prior to normalization to host time).
LOCAL_START	The local_start field contains the start of call time stamp (used for start_datime) using the local time of the re (i.e. the original start date and time prior to normalization to host time).
MANFACT	The manfact field contains the name of the manufacturer of the mobile equipment involved in this failure.
MISC1	The misc1 field contains miscellaneous information about the call failure. For SNAC OKTRs, misc1 is the Operator Voice Trunk. For DMS TCAP CFIMS, misc1 contains the error code text string. For 5ESS CIT CFIMs, misc1 indicates the stimulus for acodes CINSCTKFL, CIDSFLACP, or CIDSFLNWK. For MDIIs, misc1 contains the Local Tag for SIP calls. This indicates the Tag field from SIP-T From: or To: headers identifying this switch's side of the dialog. For REPT CELL CP FAIL messages, misc1 will contain the text used to derive the fdc. For REPT CELL HEH messages, misc1 contains the text used to derive the fdc. For E911 logs the misc1 field contains the original Emergency Service Number or the Off- Board Selective Routing (OFSBR) database information. For Alcatel Softswich CDRs, misc1 contains the interconnect facility used during the call.

Field	Description
MISC2	he misc2 field contains miscellaneous information about the call failure. For 1A ESS CFIMs, misc2 contains the special ANI information digits from the "u" field of the CIM. For 5ESS CIT CFIMs, misc2 indicates the return reason code for acode CIDSFLNWK. For MDIIs, misc2 contains the contents of the packet data indicated in the pkttype field. For DMS TCAP CFIMs, misc2 contains a three letter abbreviation of the package type from the CIM as follows: AB: Abort BEG: Begin CNP: Conversation without permission CWP: Conversation with permission END: End NIL: NIL package QWP: Query with permission QNP: Query without permission RSP: Response TCB: TC Begin TCE: TC End TCN: TC NIL package TCU: TC Unidirectional UNI: Unidirectional UNK: Unknown package type. For E911 logs the misc2 field contains the Facility Emergency Service Number (ESN).
MISC3	The misc3 field contains miscellaneous information about the call failure. For DMS TCAP CFIMs, misc3 contains the indicator, subsystem and subsystem number of the SCP application for the called address converted from hexadecimal to decimal and presented in INDICATOR-SUBSYS-SSN format. For 5ESS CIT CFIMs, misc3 represents the received message when the acode is CINCPMSG. For Autoplex REPT CELL HEH messages the misc3 field contains the number of suppressed messages by the switch. For E911 logs the misc3 field contains the AIN database Emergency Service Number (ESN).
MISC4	The misc4 field contains miscellaneous information about the call failure. For DMS TCAP CFIMs, misc4 contains the indicator, subsytem and subsystem number of the SCP application for the calling address converted from hexadecimal to decimal and presented in INDICATOR-SUBSYS-SSN format. For 5ESS CIT CFIMs, misc4 represents the command when the acode is CINCPMSG.
MISC5	The misc5 field contains miscellaneous information about the call failure. For OTR CFIMs, misc5 identifies the trunk group number used to contact the operator. For SNAC OKTRs, misc5 is the 3 port conference pack number. For AXE CDRs, misc5 contains the Bandwidth of the call. This is a single digit value with the following meaning: 0 = half rate transmission, 1 = full rate transmission, 2 = double rate transmission, 3 = triple rate transmission.

Field	Description
MISC6	The misc6 field contains miscellaneous information about the call failure. For AXE CDRs, misc6 contains the Rerouting Indicator for the call. This is a single digit value with the following meaning: 0 = no rerouting, 1 = rerouting
MSGTYPE	This is the signaling message that was involved in the failure. The message can be a SIP method, IS-41 operation, or SS7 message. For AXE CDRs, the msgtype contains Subscriber Service Indicator. This indicates which operation was invoked vis IS-41 signaling or switch feature software for this call. For REPT EVDO RNC CP FAIL messages, msgtype will contain the Error Type String, indicating the type of error being reporting in the message. For Ericsson SGSN logs this field contains the description of the log type from the log header. For HEH messages, the msgtype field contains the error type.
NREF1_ALLOCATE_1	The allocate status flag indicates the status of the PN in the active set.
NREF1_CARRIER_1	The nref1_carrier_1 field contains the first non-reference carrier channel number of the first Route Update Message for an EvDO data connection.
NREF1_CARRIER_2	The nref1_carrier_2 field contains the first non-reference carrier band class of the second Route Update Message for an EvDO data connection.
NREF1_CARRIER_BAND_1	The nref1_carrier_band_1field contains the first non- reference carrier band class of the first Route Update Message for an EvDO data connection.
NREF1_CARRIER_BAND_2	The nref1_carrier_band_2 field contains the first non- reference carrier band class of the second Route Update Message for an EvDO data connection.
NREF1_RNC_1	The nref1_rnc_1 field contains the first non-reference rnc number of the first Route Update Message for an EvDO data connection.
NREF1_RNC_2	The nref1_rnc_2 field contains the first non-reference rnc number of the second Route Update Message for an EvDO data connection.
NREF1_RT_DELAY_RES_1	The nref1_rt_delay_res_1 field indicates the roundtrip delay resolution for the first non-reference RUM record in the initial set. A value of 1 indicates that the resolution is 1/8 chip per unit, a value of 32 indicates that the resolution is 4 chips per unit.

Field	Description
NREF1_RT_DELAY_RES_2	he nref1_rt_delay_res_2 field indicates the roundtrip delay resolution for the first non-reference RUM record in the last set. A value of 1 indicates that the resolution is 1/8 chip per unit, a value of 32 indicates that the resolution is 4 chips per unit.
NREF1_SN_1	The nref1_sn_1 field contains the first non-reference PDSN number of the first Route Update Message for an EvDO data connection.
NREF1_SN_2	The nref1_sn_2 field contains the first non-reference PDSN number of the second Route Update Message for an EvDO data connection.
NREF2_ALLOCATE_1	The allocate status flag indicates the status of the PN in the active set.
NREF2_CARRIER_1	The nref2_carrier_1 field contains the second non-reference carrier channel number of the first Route Update Message for an EvDO data connection.
NREF2_CARRIER_2	The nref2_carrier_2 field contains the second non-reference carrier band class of the second Route Update Message for an EvDO data connection.
NREF2_CARRIER_BAND_1	The nref2_carrier_band_1field contains the second non-reference carrier band class of the first Route Update Message for an EvDO data connection.
NREF2_CARRIER_BAND_2	The nref2_carrier_band_2 field contains the second non-reference carrier band class of the second Route Update Message for an EvDO data connection.
NREF2_RNC_1	The nref2_rnc_1 field contains the second non-reference rnc number of the first Route Update Message for an EvDO data connection.
NREF2_RNC_2	The nref2_rnc_2 field contains the second non-reference rnc number of the second Route Update Message for an EvDO data connection.
NREF2_RT_DELAY_RES_1	The nref2_rt_delay_res_1 field indicates the roundtrip delay resolution for the second non-reference RUM record in the initial set. A value of 1 indicates that the resolution is 1/8 chip per unit, a value of 32 indicates that the resolution is 4 chips per unit.

Field	Description
NREF2_RT_DELAY_RES_2	The nref2_rt_delay_res_2 field indicates the roundtrip delay resolution for the second non-reference RUM record in the last set. A value of 1 indicates that the resolution is 1/8 chip per unit, a value of 32 indicates that the resolution is 4 chips per unit.
NREF2_SN_1	The nref2_sn_1 field contains the second non-reference PDSN number of the first Route Update Message for an EvDO data connection.
NREF2_SN_2	The nref2_sn_2 field contains the second non-reference PDSN number of the second Route Update Message for an EvDO data connection.
NREF3_ALLOCATE_1	The allocate status flag indicates the status of the PN in the active set.
NREF3_CARRIER_1	The nref3_carrier_1 field contains the third non-reference carrier channel number of the first Route Update Message for an EvDO data connection.
NREF3_CARRIER_2	The nref3_carrier_2 field contains the third non-reference carrier band class of the second Route Update Message for an EvDO data connection.
NREF3_CARRIER_BAND_1	The nref3_carrier_band_1field contains the third non- reference carrier band class of the first Route Update Message for an EvDO data connection.
NREF3_CARRIER_BAND_2	The nref3_carrier_band_2 field contains the third non-reference carrier band class of the second Route Update Message for an EvDO data connection.
NREF3_RNC_1	The nref3_rnc_1 field contains the third non-reference rnc number of the first Route Update Message for an EvDO data connection.
NREF3_RNC_2	The nref3_rnc_2 field contains the third non-reference rnc number of the second Route Update Message for an EvDO data connection.
NREF3_RT_DELAY_RES_1	The nref3_rt_delay_res_1 field indicates the roundtrip delay resolution for the third non-reference RUM record in the initial set. A value of 1 indicates that the resolution is 1/8 chip per unit, a value of 32 indicates that the resolution is 4 chips per unit.

Field	Description
NREF3_RT_DELAY_RES_2	The nref3_rt_delay_res_2 field indicates the roundtrip delay resolution for the third non-reference RUM record in the last set. A value of 1 indicates that the resolution is 1/8 chip per unit, a value of 32 indicates that the resolution is 4 chips per unit.
NREF3_SN_1	The nref3_sn_1 field contains the third non-reference PDSN number of the first Route Update Message for an EvDO data connection.
NREF3_SN_2	The nref3_sn_2 field contains the third non-reference PDSN number of the second Route Update Message for an EvDO data connection.
NREF4_ALLOCATE_1	The allocate status flag indicates the status of the PN in the active set.
NREF4_CARRIER_1	The nref4_carrier_1 field contains the fourth non-reference carrier channel number of the first Route Update Message for an EvDO data connection.
NREF4_CARRIER_2	The nref4_carrier_2 field contains the fourth non-reference carrier band class of the second Route Update Message for an EvDO data connection.
NREF4_CARRIER_BAND_1	The nref4_carrier_band_1 field contains the fourth non-reference carrier band class of the first Route Update Message for an EvDO data connection.
NREF4_CARRIER_BAND_2	The nref4_carrier_band_2 field contains the fourth non-reference carrier band class of the second Route Update Message for an EvDO data connection.
NREF4_RNC_1	The nref4_rnc_1field contains the fourth non-reference rnc number of the first Route Update Message for an EvDO data connection.
NREF4_RNC_2	The nref4_rnc_2 field contains the fourth non-reference rnc number of the second Route Update Message for an EvDO data connection.
NREF4_RT_DELAY_RES_1	The nref4_rt_delay_res_1 field indicates the roundtrip delay resolution for the fourth non-reference RUM record in the initial set. A value of 1 indicates that the resolution is 1/8 chip per unit, a value of 32 indicates that the resolution is 4 chips per unit.

Field	Description
NREF4_RT_DELAY_RES_2	The nref4_rt_delay_res_2 field indicates the roundtrip delay resolution for the fourth non-reference RUM record in the last set. A value of 1 indicates that the resolution is 1/8 chip per unit, a value of 32 indicates that the resolution is 4 chips per unit.
NREF4_SN_1	The nref4_sn_1 field contains the fourth non-reference PDSN number of the first Route Update Message for an EvDO data connection.
NREF4_SN_2	The nref4_sn_2 field contains the fourth non-reference PDSN number of the second Route Update Message for an EvDO data connection.
NREF5_ALLOCATE_1	The allocate status flag indicates the status of the PN in the active set.
NREF5_CARRIER_1	The nref5_carrier_1 field contains the fifth non-reference carrier channel number of the first Route Update Message for an EvDO data connection.
NREF5_CARRIER_2	The nref5_carrier_2 field contains the fifth non-reference carrier band class of the second Route Update Message for an EvDO data connection.
NREF5_CARRIER_BAND_1	The nref5_carrier_band_1field contains the fifth non- reference carrier band class of the first Route Update Message for an EvDO data connection.
NREF5_CARRIER_BAND_2	The nref5_carrier_band_2 field contains the fifth non- reference carrier band class of the second Route Update Message for an EvDO data connection.
NREF5_RNC_1	The nref5_rnc_1 field contains the fifth non-reference rnc number of the first Route Update Message for an EvDO data connection.
NREF5_RNC_2	The nref5_rnc_2 field contains the fifth non-reference rnc number of the second Route Update Message for an EvDO data connection.
NREF5_RT_DELAY_RES_1	The nref5_rt_delay_res_1 field indicates the roundtrip delay resolution for the fifth non-reference RUM record in the initial set. A value of 1 indicates that the resolution is 1/8 chip per unit, a value of 32 indicates that the resolution is 4 chips per unit.

Field	Description
NREF5_RT_DELAY_RES_2	The nref5_rt_delay_res_2 field indicates the roundtrip delay resolution for the fifth non-reference RUM record in the last set. A value of 1 indicates that the resolution is 1/8 chip per unit, a value of 32 indicates that the resolution is 4 chips per unit.
NREF5_SN_1	The nref5_sn_1 field contains the fifth non-reference PDSN number of the first Route Update Message for an EvDO data connection.
NREF5_SN_2	The nref5_sn_2 field contains the fifth non-reference PDSN number of the second Route Update Message for an EvDO data connection.
NREF1_NET_EFF_LOAD_1	The Network Effective Load field reports the filtered value for Network Effective (Neff) Load for this Pilot that is used by the Network Load Balancing Evaluation. It is included only when there is a valid Neff value available for this Pilot, otherwise this field is Null. For the first RUM, this field is only populated for those Pilots included in the active set that is assigned during the connection setup procedure for which valid Neff values are available. For the last RUM, this field is only populated for those Pilots included in the last active set of the connection for which valid Neff values are available. This field is in 1/16 linear dimensionless units with a lower value corresponding to lower loading. This field must be divided by 16 to obtain the value of NEFF.
NREF2_NET_EFF_LOAD_1	The Network Effective Load field reports the filtered value for Network Effective (Neff) Load for this Pilot that is used by the Network Load Balancing Evaluation. It is included only when there is a valid Neff value available for this Pilot, otherwise this field is Null. For the first RUM, this field is only populated for those Pilots included in the active set that is assigned during the connection setup procedure for which valid Neff values are available. For the last RUM, this field is only populated for those Pilots included in the last active set of the connection for which valid Neff values are available. This field is in 1/16 linear dimensionless units with a lower value corresponding to lower loading. This field must be divided by 16 to obtain the value of NEFF.

Field	Description
NREF3_NET_EFF_LOAD_1	The Network Effective Load field reports the filtered value for Network Effective (Neff) Load for this Pilot that is used by the Network Load Balancing Evaluation. It is included only when there is a valid Neff value available for this Pilot, otherwise this field is Null. For the first RUM, this field is only populated for those Pilots included in the active set that is assigned during the connection setup procedure for which valid Neff values are available. For the last RUM, this field is only populated for those Pilots included in the last active set of the connection for which valid Neff values are available. This field is in 1/16 linear dimensionless units with a lower value corresponding to lower loading. This field must be divided by 16 to obtain the value of NEFF.
NREF4_NET_EFF_LOAD_1	The Network Effective Load field reports the filtered value for Network Effective (Neff) Load for this Pilot that is used by the Network Load Balancing Evaluation. It is included only when there is a valid Neff value available for this Pilot, otherwise this field is Null. For the first RUM, this field is only populated for those Pilots included in the active set that is assigned during the connection setup procedure for which valid Neff values are available. For the last RUM, this field is only populated for those Pilots included in the last active set of the connection for which valid Neff values are available. This field is in 1/16 linear dimensionless units with a lower value corresponding to lower loading. This field must be divided by 16 to obtain the value of NEFF.
NREF5_NET_EFF_LOAD_1	The Network Effective Load field reports the filtered value for Network Effective (Neff) Load for this Pilot that is used by the Network Load Balancing Evaluation. It is included only when there is a valid Neff value available for this Pilot, otherwise this field is Null. For the first RUM, this field is only populated for those Pilots included in the active set that is assigned during the connection setup procedure for which valid Neff values are available. For the last RUM, this field is only populated for those Pilots included in the last active set of the connection for which valid Neff values are available. This field is in 1/16 linear dimensionless units with a lower value corresponding to lower loading. This field must be divided by 16 to obtain the value of NEFF.

Field	Description
NREF1_NET_EFF_LOAD_2	The Network Effective Load field reports the filtered value for Network Effective (Neff) Load for this Pilot that is used by the Network Load Balancing Evaluation. It is included only when there is a valid Neff value available for this Pilot, otherwise this field is Null. For the first RUM, this field is only populated for those Pilots included in the active set that is assigned during the connection setup procedure for which valid Neff values are available. For the last RUM, this field is only populated for those Pilots included in the last active set of the connection for which valid Neff values are available. This field is in 1/16 linear dimensionless units with a lower value corresponding to lower loading. This field must be divided by 16 to obtain the value of NEFF.
NREF2_NET_EFF_LOAD_2	The Network Effective Load field reports the filtered value for Network Effective (Neff) Load for this Pilot that is used by the Network Load Balancing Evaluation. It is included only when there is a valid Neff value available for this Pilot, otherwise this field is Null. For the first RUM, this field is only populated for those Pilots included in the active set that is assigned during the connection setup procedure for which valid Neff values are available. For the last RUM, this field is only populated for those Pilots included in the last active set of the connection for which valid Neff values are available. This field is in 1/16 linear dimensionless units with a lower value corresponding to lower loading. This field must be divided by 16 to obtain the value of NEFF.
NREF3_NET_EFF_LOAD_2	The Network Effective Load field reports the filtered value for Network Effective (Neff) Load for this Pilot that is used by the Network Load Balancing Evaluation. It is included only when there is a valid Neff value available for this Pilot, otherwise this field is Null. For the first RUM, this field is only populated for those Pilots included in the active set that is assigned during the connection setup procedure for which valid Neff values are available. For the last RUM, this field is only populated for those Pilots included in the last active set of the connection for which valid Neff values are available. This field is in 1/16 linear dimensionless units with a lower value corresponding to lower loading. This field must be divided by 16 to obtain the value of NEFF.

Field	Description
NREF4_NET_EFF_LOAD_2	The Network Effective Load field reports the filtered value for Network Effective (Neff) Load for this Pilot that is used by the Network Load Balancing Evaluation. It is included only when there is a valid Neff value available for this Pilot, otherwise this field is Null. For the first RUM, this field is only populated for those Pilots included in the active set that is assigned during the connection setup procedure for which valid Neff values are available. For the last RUM, this field is only populated for those Pilots included in the last active set of the connection for which valid Neff values are available. This field is in 1/16 linear dimensionless units with a lower value corresponding to lower loading. This field must be divided by 16 to obtain the value of NEFF.
NREF5_NET_EFF_LOAD_2	The Network Effective Load field reports the filtered value for Network Effective (Neff) Load for this Pilot that is used by the Network Load Balancing Evaluation. It is included only when there is a valid Neff value available for this Pilot, otherwise this field is Null. For the first RUM, this field is only populated for those Pilots included in the active set that is assigned during the connection setup procedure for which valid Neff values are available. For the last RUM, this field is only populated for those Pilots included in the last active set of the connection for which valid Neff values are available. This field is in 1/16 linear dimensionless units with a lower value corresponding to lower loading. This field must be divided by 16 to obtain the value of NEFF.
NUM_PAGES	The num_pages field indicates the number of CDMA pages.
NUM_QOS_PG	The num_qos_pg field contains the number of QOS pages for the EvDO connection.
NUMD	The numd field specifies the number of digits in the digits field of the CFIM.
O_IP	The o_ip field contains the ip address of the egress gateway or terminating side.
OBYTE	The obyte field contains the byte count for the session from the ingress to egress side. For AnyPath(R) CDRs, this field contains the total length of the message in bytes.
OBYTE_RETRANS	The obyte_retrans field contains the number of outbound (uplink) bytes that were retransmitted during the connection.
OGT	The ogt field contains the outgoing trunk group member for the call.

Field	Description
OTGID	The otgid field contains the outgoing trunk group for the call.
P	The pegging status (p) field will be "y" if the CFIM is used as input into thresholding and alerting. This field has the value "n" if the CFIM was disabled from thresholding and alerting because the FDC and digits fields in the CFIM matched an FDC and digit pattern in the disabledig table. The disabling of CFIMs based on FDC and digits is an optional feature.
PERS_TYPE	The personality type contains configuration information for the EvDO data connection. Values are: 0 - Rev 0 1 - Basic Rev A (no Multi-Flow), 2 - Rev A with Multi-Flow.
PG_PROFID	The pg_profid field contains the paging profile ID for the EvDO connection.
PROTOCOL	The protocol field contains information about the protocol involved in the failure. For EvDO CP Fail messages it contains the Protocol Subtypes for session release due to security parameter inconsistencies.
PSMM_AGG_PILOT_STR_1	Aggregate pilot strength of: psmm_ref1_pilot_str_1, psmm_nref1_pilot_str_1, psmm_nref2_pilot_str_1, psmm_nref3_pilot_str_1, psmm_nref4_pilot_str_1 and psmm_nref5_pilot_str_1
PSMM_AGG_PILOT_STR_2	Aggregate pilot strength of: psmm_ref1_pilot_str_2, psmm_nref1_pilot_str_2, psmm_nref2_pilot_str_2, psmm_nref3_pilot_str_2, psmm_nref4_pilot_str_2 and psmm_nref5_pilot_str_2.
PSMM_NREF1_AS_POST_1	The psmm_nref1_as_post_1 field contains the first non-reference post-handoff evaluation of the first Route Update Message for an EvDO data connection.
PSMM_NREF1_AS_POST_2	The psmm_nref1_as_post_2 field contains the first non-reference post-handoff evaluation of the second Route Update Message for an EvDO data connection.
PSMM_NREF1_AS_PRE_1	The psmm_nref1_as_pre_1 field contains the first non-reference pre-handoff evaluation of the first Route Update Message for an EvDO data connection.
PSMM_NREF1_AS_PRE_2	The psmm_nref1_as_pre_2 field contains the first non-reference pre-handoff evaluation of the second Route Update Message for an EvDO data connection.
PSMM_NREF1_CELL_1	The psmm_nref1_cell_1 field contains the first non-reference cell number of the first Route Update Message for an EvDO data connection.

Field	Description
PSMM_NREF1_CELL_2	The psmm_nref1_cell_2 field contains the first non-reference cell number of the second Route Update Message for an EvDO data connection.
PSMM_NREF1_HO_COMP_1	The psmm_nref1_ho_comp_1 field indicates whether a traffic channel confirmation was received after a handoff success for the active set.
PSMM_NREF1_HO_COMP_2	The psmm_nref1_ho_comp_2 field indicates whether a traffic channel confirmation was received after a handoff success for the active set.
PSMM_NREF1_KEEP_IND_1	The psmm_nref1_keep_ind_1 field contains the first non-reference keep indicator of the first Route Update Message for an EvDO data connection.
PSMM_NREF1_KEEP_IND_2	The psmm_nref1_keep_ind_2 field contains the first non-reference keep indicator of the second Route Update Message for an EvDO data connection.
PSMM_NREF1_PILOT_STR_1	The psmm_nref1_pilot_str_1 field contains the pilot strength at the AT for the cell. The psmm_nref1_pilot_str_1 field can range from 0 to 99.
PSMM_NREF1_PILOT_STR_2	The psmm_nref1_pilot_str_2 field contains the pilot strength at the AT for the first non-reference cell of the second Route Update Message for an EvDO data connection.
PSMM_NREF1_PN_PHASE_1	The psmm_nref1_pn_phase_1 field contains the first non-reference phase of pilot PN sequence.
PSMM_NREF1_PN_PHASE_2	The psmm_nref1_pn_phase_2 field contains the first non-reference Pseudo-Noise offset of the second Route Update Message for an EvDO data connection.
PSMM_NREF1_RT_DELAY_1	The psmm_nref1_rt_delay_1 field contains the round delay for the cell.
PSMM_NREF1_RT_DELAY_2	The psmm_nref1_rt_delay_2 field contains the round trip delay for the first non-reference cell of the second Route Update Message for an EvDO data connection.
PSMM_NREF1_SECTOR_1	The psmm_nref1_sector_1 field contains the first non-reference sector number of the first Route Update Message for an EvDO data connection.
PSMM_NREF1_SECTOR_2	The psmm_nref1_sector_2 field contains the first non-reference sector number of the second Route Update Message for an EvDO data connection

Field	Description
PSMM_NREF2_AS_POST_1	he psmm_nref2_as_post_1 field contains the second non-reference post-handoff evaluation of the first Route Update Message for an EvDO data connection.
PSMM_NREF2_AS_POST_2	The psmm_nref2_as_post_2 field contains the second non-reference post-handoff evaluation of the second Route Update Message for an EvDO data connection.
PSMM_NREF2_AS_PRE_1	The psmm_nref2_as_pre_1 field contains the second non-reference pre-handoff evaluation of the first Route Update Message for an EvDO data connection.
PSMM_NREF2_AS_PRE_2	The psmm_nref2_as_pre_2 field contains the second non-reference pre-handoff evaluation of the second Route Update Message for an EvDO data connection.
PSMM_NREF2_CELL_1	The psmm_nref2_cell_1 field contains the second non-reference cell number of the first Route Update Message for an EvDO data connection.
PSMM_NREF2_CELL_2	The psmm_nref2_cell_2 field contains the second non-reference cell number of the second Route Update Message for an EvDO data connection.
PSMM_NREF2_HO_COMP_1	The psmm_nref2_ho_comp_1 field indicates whether a traffic channel confirmation was received after a handoff success for the active set.
PSMM_NREF2_HO_COMP_2	The psmm_nref2_ho_comp_2 field indicates whether a traffic channel confirmation was received after a handoff success for the active set.
PSMM_NREF2_KEEP_IND_1	The psmm_nref2_keep_ind_1 field contains the second non-reference keep indicator of the first Route Update Message for an EvDO data connection.
PSMM_NREF2_KEEP_IND_2	The psmm_nref2_keep_ind_2 field contains the second non-reference keep indicator of the second Route Update Message for an EvDO data connection.
PSMM_NREF2_PILOT_STR_1	The psmm_nref2_pilot_str_1 field contains the pilot strength at the AT for the cell.
PSMM_NREF2_PILOT_STR_2	The psmm_nref2_pilot_str_2 field contains the pilot strength at the AT for the second non-reference cell of the second Route Update Message for an EvDO data connection.
PSMM_NREF2_PN_PHASE_1	The psmm_nref2_pn_phase_1 field contains the second non-reference phase of pilot PN sequence.

Field	Description
PSMM_NREF2_PN_PHASE_2	The psmm_nref2_pn_phase_2 field contains the second non-reference Pseudo-Noise offset of the second Route Update Message for an EvDO data connection.
PSMM_NREF2_RT_DELAY_1	The psmm_nref2_rt_delay_1 field contains the round delay for the cell.
PSMM_NREF2_RT_DELAY_2	The psmm_nref2_rt_delay_2 field contains the round trip delay for the second non-reference cell of the second Route Update Message for an EvDO data connection.
PSMM_NREF2_SECTOR_1	The psmm_nref2_sector_1 field contains the second non-reference sector number of the first Route Update Message for an EvDO data connection.
PSMM_NREF2_SECTOR_2	The psmm_nref2_sector_2 field contains the second non-reference sector number of the second Route Update Message for an EvDO data connection.
PSMM_NREF3_AS_POST_1	The psmm_nref3_as_post_1 field contains the third non-reference post-handoff evaluation of the first Route Update Message for an EvDO data connection.
PSMM_NREF3_AS_POST_2	The psmm_nref3_as_post_2 field contains the third non-reference post-handoff evaluation of the second Route Update Message for an EvDO data connection.
PSMM_NREF3_AS_PRE_1	The psmm_nref3_as_pre_1 field contains the third non-reference pre-handoff evaluation of the first Route Update Message for an EvDO data connection.
PSMM_NREF3_AS_PRE_2	The psmm_nref3_as_pre_2 field contains the third non-reference pre-handoff evaluation of the second Route Update Message for an EvDO data connection.
PSMM_NREF3_CELL_1	The psmm_nref3_cell_1 field contains the third non-reference cell number of the first Route Update Message for an EvDO data connection.
PSMM_NREF3_CELL_2	The psmm_nref3_cell_2 field contains the third non-reference cell number of the second Route Update Message for an EvDO data connection.
PSMM_NREF3_HO_COMP_1	The psmm_nref3_ho_comp_1 field indicates whether a traffic channel confirmation was received after a handoff success for the active set.
PSMM_NREF3_HO_COMP_2	The psmm_nref3_ho_comp_2 field indicates whether a traffic channel confirmation was received after a handoff success for the active set.

Field	Description
PSMM_NREF3_KEEP_IND_1	The psmm_nref3_keep_ind_1 field contains the third non-reference keep indicator of the first Route Update Message for an EvDO data connection.
PSMM_NREF3_KEEP_IND_2	The psmm_nref3_keep_ind_2 field contains the third non-reference keep indicator of the second Route Update Message for an EvDO data connection.
PSMM_NREF3_PILOT_STR_1	The psmm_nref3_pilot_str_1 field contains the pilot strength at the AT for the cell.
PSMM_NREF3_PILOT_STR_2	The psmm_nref3_pilot_str_2 field contains the pilot strength at the AT for the third non-reference cell of the second Route Update Message for an EvDO data connection.
PSMM_NREF3_PN_PHASE_1	The psmm_nref3_pn_phase_1 field contains the third non-reference phase of pilot PN sequence.
PSMM_NREF3_PN_PHASE_2	The psmm_nref3_pn_phase_2 field contains the third non-reference Pseudo-Noise offset of the second Route Update Message for an EvDO data connection.
PSMM_NREF3_RT_DELAY_1	The psmm_nref3_rt_delay_1 field contains the round delay for the cell. The psmm_nref3_rt_delay_1 field can range from 0 to 99999.
PSMM_NREF3_RT_DELAY_2	The psmm_nref3_rt_delay_2 field contains the round trip delay for the third non-reference cell of the second Route Update Message for an EvDO data connection.
PSMM_NREF3_SECTOR_1	The psmm_nref3_sector_1 field contains the third non-reference sector number of the first Route Update Message for an EvDO data connection.
PSMM_NREF3_SECTOR_2	The psmm_nref3_sector_2 field contains the third non-reference sector number of the second Route Update Message for an EvDO data connection.
PSMM_NREF4_AS_POST_1	The psmm_nref4_as_post_1 field contains the fourth non-reference post-handoff evaluation er of the first Route Update Message for an EvDO data connection.
PSMM_NREF4_AS_POST_2	The psmm_nref4_as_post_2 field contains the fourth non-reference post-handoff evaluation er of the second Route Update Message for an EvDO data connection.
PSMM_NREF4_AS_PRE_1	The psmm_nref4_as_pre_1 field contains the fourth non-reference pre-handoff evaluation er of the first Route Update Message for an EvDO data connection.

Field	Description
PSMM_NREF4_AS_PRE_2	The psmm_nref4_as_pre_2 field contains the fourth non-reference pre-handoff evaluation er of the second Route Update Message for an EvDO data connection.
PSMM_NREF4_CELL_1	The psmm_nref4_cell_1 field contains the fourth non-reference cell number of the first Route Update Message for an EvDO data connection.
PSMM_NREF4_CELL_2	The psmm_nref4_cell_2 field contains the fourth non-reference cell number of the second Route Update Message for an EvDO data connection.
PSMM_NREF4_HO_COMP_1	The psmm_nref4_ho_comp_1 field indicates whether a traffic channel confirmation was received after a handoff success for the active set.
PSMM_NREF4_HO_COMP_2	The psmm_nref4_ho_comp_2 field indicates whether a traffic channel confirmation was received after a handoff success for the active set.
PSMM_NREF4_KEEP_IND_1	The psmm_nref4_keep_ind_1 field contains the fourth non-reference keep indicator of the first Route Update Message for an EvDO data connection.
PSMM_NREF4_KEEP_IND_2	The psmm_nref4_keep_ind_2 field contains the fourth non-reference keep indicator of the second Route Update Message for an EvDO data connection.
PSMM_NREF4_PILOT_STR_1	The psmm_nref4_pilot_str_1 field contains the pilot strength at the AT for the cell.
PSMM_NREF4_PILOT_STR_2	The psmm_nref4_pilot_str_2 field contains the pilot strength at the AT for the fourth non-reference cell of the second Route Update Message for an EvDO data connection.
PSMM_NREF4_PN_PHASE_1	The psmm_nref4_pn_phase_1 field contains the fourth non-reference phase of pilot PN sequence.
PSMM_NREF4_PN_PHASE_2	The psmm_nref4_pn_phase_2 field contains the fourth non-reference Pseudo-Noise offset of the second Route Update Message for an EvDO data connection.
PSMM_NREF4_RT_DELAY_1	The psmm_nref4_rt_delay_1 field contains the round delay for the cell.
PSMM_NREF4_RT_DELAY_2	The psmm_nref4_rt_delay_2 field contains the round trip delay for the fourth non-reference cell of the second Route Update Message for an EvDO data connection.

Field	Description
PSMM_NREF4_SECTOR_1	The psmm_nref4_sector_1 field contains the fourth non-reference sector number of the first Route Update Message for an EvDO data connection.
PSMM_NREF4_SECTOR_2	The psmm_nref4_sector_2 field contains the fourth non-reference sector number of the second Route Update Message for an EvDO data connection.
PSMM_NREF5_AS_POST_1	The psmm_nref5_as_post_1 field contains the fifth non-reference post-handoff evaluation of the first Route Update Message for an EvDO data connection.
PSMM_NREF5_AS_POST_2	The psmm_nref5_as_post_2 field contains the fifth non-reference post-handoff evaluation of the second Route Update Message for an EvDO data connection.
PSMM_NREF5_AS_PRE_1	The psmm_nref5_as_pre_1 field contains the fifth non-reference pre-handoff evaluation of the first Route Update Message for an EvDO data connection.
PSMM_NREF5_AS_PRE_2	The psmm_nref5_as_pre_2 field contains the fifth non-reference pre-handoff evaluation of the second Route Update Message for an EvDO data connection.
PSMM_NREF5_CELL_1	The psmm_nref5_cell_1 field contains the fifth non-reference cell number of the first Route Update Message for an EvDO data connection.
PSMM_NREF5_CELL_2	The psmm_nref5_cell_2 field contains the fifth non-reference cell number of the second Route Update Message for an EvDO data connection.
PSMM_NREF5_HO_COMP_1	The psmm_nref5_ho_comp_1 field indicates whether a traffic channel confirmation was received after a handoff success for the active set.
PSMM_NREF5_HO_COMP_2	The psmm_nref5_ho_comp_2 field indicates whether a traffic channel confirmation was received after a handoff success for the active set.
PSMM_NREF5_KEEP_IND_1	The psmm_nref5_keep_ind_1 field contains the fifth non-reference keep indicator of the first Route Update Message for an EvDO data connection.
PSMM_NREF5_KEEP_IND_2	The psmm_nref5_keep_ind_2 field contains the fifth non-reference keep indicator of the second Route Update Message for an EvDO data connection.
PSMM_NREF5_PILOT_STR_1	The psmm_nref5_pilot_str_1 field contains the pilot strength at the AT for the cell.

Field	Description
PSMM_NREF5_PILOT_STR_2	The psmm_nref5_pilot_str_2 field contains the pilot strength at the AT for the fifth non-reference cell of the second Route Update Message for an EvDO data connection.
PSMM_NREF5_PN_PHASE_1	The psmm_nref5_pn_phase_1 field contains the fifth non-reference phase of pilot PN sequence.
PSMM_NREF5_PN_PHASE_2	The psmm_nref5_pn_phase_2 field contains the fifth non-reference Pseudo-Noise offset of the second Route Update Message for an EvDO data connection.
PSMM_NREF5_RT_DELAY_1	The psmm_nref5_rt_delay_1 field contains the round delay for the cell.
PSMM_NREF5_RT_DELAY_2	The psmm_nref5_rt_delay_2 field contains the round trip delay for the fifth non-reference cell of the second Route Update Message for an EvDO data connection.
PSMM_NREF5_SECTOR_1	The psmm_nref5_sector_1 field contains the fifth non-reference sector number of the first Route Update Message for an EvDO data connection.
PSMM_NREF5_SECTOR_2	The psmm_nref5_sector_2 field contains the fifth non-reference sector number of the second Route Update Message for an EvDO data connection.
PSMM_REF1_AS_POST_1	The psmm_ref1_as_post_1 field contains the reference post-handoff evaluation of the first Route Update Message for an EvDO data connection.
PSMM_REF1_AS_POST_2	The psmm_ref1_as_post_2 field contains the reference post-handoff evaluation of the second Route Update Message for an EvDO data connection.
PSMM_REF1_AS_PRE_1	The psmm_ref1_as_pre_1 field contains the reference pre-handoff evaluation of the first Route Update Message for an EvDO data connection.
PSMM_REF1_AS_PRE_2	The psmm_ref1_as_pre_2 field contains the reference pre-handoff evaluation of the second Route Update Message for an EvDO data connection.
PSMM_REF1_CARRIER_1	The psmm_ref1_carrier_1 field contains the reference CDMA carrier number.
PSMM_REF1_CARRIER_2	The psmm_ref1_carrier_2 field contains the reference CDMA carrier number.

Field	Description
PSMM_REF1_CELL_1	The psmm_ref1_cell_1 field contains the reference cell number of the first Route Update Message for an EvDO data connection. The psmm_ref1_cell_1 field contains the identity of reference cell site.
PSMM_REF1_CELL_2	The psmm_ref1_cell_2 field contains the reference cell number of the second Route Update Message for an EvDO data connection.
PSMM_REF1_HO_1	The psmm_ref1_ho_1 flag indicates the handoff activity caused by the first Route Update Message. Values are: 0 - No Handoff activity, 1 - Add a call leg to the active set, 2 - Drop a call leg to the active set, 3 - Add/Drop one leg at the same time, 4 - AT-Assisted IFHO 5 - Directed IFHO
PSMM_REF1_HO_2	The psmm_ref1_ho_2 flag indicates the handoff activity caused by the last Route Update Message. Values are: 0 - No Handoff activity, 1 - Add a call leg to the active set, 2 - Drop a call leg to the active set, 3 - Add/Drop one leg at the same time, 4 - AT-Assisted IFHO, 5 - Directed IFHO
PSMM_REF1_HO_COMP_1	The psmm_ref1_ho_comp_1 field indicates whether a traffic channel confirmation was received after a handoff success for the active set.
PSMM_REF1_HO_COMP_2	The psmm_ref1_ho_comp_2 field indicates whether a traffic channel confirmation was received after a handoff success for the active set.
PSMM_REF1_KEEP_IND_1	The psmm_ref1_keep_ind_1 field contains the reference keep indicator of the first Route Update Message for an EvDO data connection.
PSMM_REF1_KEEP_IND_2	The psmm_ref1_keep_ind_2 field contains the reference keep indicator of the second Route Update Message for an EvDO data connection.
PSMM_REF1_NUM_PILOTS_1	The psmm_ref1_num_pilots_1 field contains the number of pilots for the reference set. The psmm_ref1_num_pilots_1 field can range from 0 to 6.
PSMM_REF1_NUM_PILOTS_2	The psmm_ref1_num_pilots_2 field contains the number of pilots for the reference set. The psmm_ref1_num_pilots_2 field can range from 0 to 6.
PSMM_REF1_PILOT_STR_1	The psmm_ref1_pilot_str_1 field contains the pilot strength at the AT for the cell.

Field	Description
PSMM_REF1_PILOT_STR_2	The psmm_ref1_pilot_str_2 field contains the pilot strength at the AT for the reference cell of the second Route Update Message for an EvDO data connection.
PSMM_REF1_PN_OFFSET_1	The psmm_ref1_pn_offset_1 field contains the Pseudo-Noise offset.
PSMM_REF1_PN_OFFSET_2	The psmm_ref1_pn_offset_2 field contains the Pseudo-Noise offset.
PSMM_REF1_PN_PHASE_1	The psmm_ref1_pn_phase_1 field contains reference phase of pilot Pseudo Noise sequence.
PSMM_REF1_RT_DELAY_1	The psmm_ref1_rt_delay_1 field contains the round delay for the cell.
PSMM_REF1_RT_DELAY_2	The psmm_ref1_rt_delay_2 field contains the round trip delay for the reference cell of the second Route Update Message for an EvDO data connection.
PSMM_REF1_SECTOR_1	The psmm_ref1_sector_1 field contains the reference sector number of the first Route Update Message for an EvDO data connection. The psmm_ref1_sector_1 field contains the identity of sector on the reference cell.
PSMM_REF1_SECTOR_2	The psmm_ref1_sector_2 field contains the reference sector number of the second Route Update Message for an EvDO data connection.
PSMM_REF1_TIMESTAMP_1	The psmm_ref1_timestamp_1 field contains the timestamp of the first Route Update Message for an EvDO data connection.
PSMM_REF1_TIMESTAMP_2	The psmm_ref1_timestamp_2 field contains the timestamp of the last Route Update Message for an EvDO data connection.
R	The related direction (r) indicates, relative to the RE, the direction of the trunk connecting the RE and the entity identified in the related field.
RATI	The rati field contains the random access terminal identifier in a session setup attempt.
RE	The reporting entity (re) is the entity that forwarded the CIM or the switching office determined to be the origination of the call.
REASON	This is the reason text for the failure. For REPT CELL HEH messages, reason field contains the additional error information text.

Field	Description
REASON2	The reason2 field contains secondary failure reason text. It is intended to supplement the reason field. For HEH messages, the reason2 field contains a combination of hardware status and CLGC information.
REC_CREATE_TIME	The rec_create_time is the Record Creation Timestamp (field 79) in EvDO PCMD record. It will be converted from milliseconds to a datime with field 3 (Month and Day).
REF1_ALLOCATE_1	The allocate status flag indicates the status of the PN in the active set.
REF1_CARRIER_BAND_1	The ref1_carrier_band_1field contains the reference carrier band class of the first Route Update Message for an EvDO data connection.
REF1_CARRIER_BAND_2	The ref1_carrier_band_2 field contains the reference carrier band class of the second Route Update Message for an EvDO data connection.
REF1_NET_EFF_LOAD_1	The Network Effective Load field reports the filtered value for Network Effective (Neff) Load for this Pilot that is used by the Network Load Balancing Evaluation. It is included only when there is a valid Neff value available for this Pilot, otherwise this field is Null. For the first RUM, this field is only populated for those Pilots included in the active set that is assigned during the connection setup procedure for which valid Neff values are available. For the last RUM, this field is only populated for those Pilots included in the last active set of the connection for which valid Neff values are available. This field is in 1/16 linear dimensionless units with a lower value corresponding to lower loading. This field must be divided by 16 to obtain the value of NEFF.
REF1_NET_EFF_LOAD_2	The Network Effective Load field reports the filtered value for Network Effective (Neff) Load for this Pilot that is used by the Network Load Balancing Evaluation. It is included only when there is a valid Neff value available for this Pilot, otherwise this field is Null. For the first RUM, this field is only populated for those Pilots included in the active set that is assigned during the connection setup procedure for which valid Neff values are available. For the last RUM, this field is only populated for those Pilots included in the last active set of the connection for which valid Neff values are available. This field is in 1/16 linear dimensionless units with a lower value corresponding to lower loading. This field must be divided by 16 to obtain the value of NEFF.

Field	Description
REF1_RNC_1	The ref1_rnc_1 field contains the reference rnc number of the first Route Update Message for an EvDO data connection.
REF1_RNC_2	The ref1_rnc_2 field contains the reference rnc number of the second Route Update Message for an EvDO data connection.
REF1_RT_DELAY_RES_1	The ref1_rt_delay_res_1 field indicates the roundtrip delay resolution for the reference RUM record in the initial set. A value of 1 indicates that the resolution is 1/8 chip per unit, a value of 32 indicates that the resolution is 4 chips per unit.
REF1_RT_DELAY_RES_2	The ref1_rt_delay_res_2 field indicates the roundtrip delay resolution for the reference RUM record in the last set. A value of 1 indicates that the resolution is 1/8 chip per unit, a value of 32 indicates that the resolution is 4 chips per unit.
REF1_SN_1	The ref1_sn_1 field contains the reference PDSN number of the first Route Update Message for an EvDO data connection.
REF1_SN_2	The nref1_sn_2 field contains the reference PDSN number of the second Route Update Message for an EvDO data connection.
RELATED	The related entity field (related) contains the CLLI code of the related entity or reporting entity.
RETYPE	The reporting entity type (retype) field contains the equipment type for the reporting entity. This field is validated against the type field of the eqtype table.
RL_SUBPKTS	The RL Subpackets field contains the number of subpackets for all RL bearer traffic serving the connection. It is the actual number of subpackets received on the reverse traffic channels. Post-processing tools can calculate RL RLP Throughput in bytes per second as RL RLP Bytes / RL Active Duration, where RL RLP Bytes is field 46 and RL Active Duration is RL Subpackets * 0.0067 seconds.
RNC	The rnc field contains the identifier for the Radio Network Controller.
RS	The reporting office home STP (rs) field contains the home STP pair of the reporting office. A "?" in this field indicates an STP was involved in the call but the identity of the STP is unknown to the system. A "-" in this field indicates that no STP was involved in the call which used in-band or non-SS7 signaling. This value must have been a ne entry in the stparch table.

Field	Description
RT_DELAY	The rt_delay is the Access Round Trip Delay (field 60) in the EvDO PCMD record.
RT_DELAY_RES	The rt_delay_res field indicates the roundtrip delay resolution for the EvDO PCMD record. A value of 1 indicates that the resolution is 1/8 chip per unit, a value of 32 indicates that the resolution is 4 chips per unit.
S	The status (s) field indicates the status of the call irregularity being reported.
SECTOR	The sector field represents the initial secor number. "-" is a valid value that indicates the field is not applicable or there is no data available.
SEIZ_BAND	The seiz_band field contains the carrier band class at the time of connection seizure.
SEIZ_CHAN	The seiz_chan field contains the channel number at the time of connection seizure.
SERNO	The serial number field provides the serial number of the mobile unit involved with a call. This field can be an ESN for CDMA, or an IMEI for GSM.
SERV_NODE	The serv_node field contains the service node identifier for the message. For EvDO CP Fail and EvDO PCMD messages, this is the OMP identifier.
SESS_CAUS	The sess_caus is the Session Setup Final Class Qualifier (field 89) in the EvDO PCMD record.
SESS_COMP	The sess_comp field contains the timestamp indicating when the session was completed.
SESS_SEC	The Session Security field indicates whether security is activated for this session. 0 = Security not activated, 1 = Security activated
SESS_START	The sess_start field contains the timestamp indicating when the session was started.
SESS_TYPE	The sess_type field indicates the type of session that was requested.
SIG	The signaling (sig) field indicates the type of signaling involved in the irregularity. It is used by the system so as not to peg an STP for irregularities with in-band and other non-SS7 signaling. This field is validated against the type field of the signaling table.
SILENT_REORIG	he silent_reorig field contains the silent re-origination flag.

Field	Description
SM_CNT1	The sm_cnt1 field contains the service measurement 1 count.
SM_CNT2	The sm_cnt2 field contains the service measurement 2 count.
SM_CNT3	The sm_cnt3 field contains the service measurement 3 count.
SM_CNT4	The sm_cnt4 field contains the service measurement 4 count.
SM_CNT5	The sm_cnt5 field contains the service measurement 5 count.
SM_CNT6	The sm_cnt6 field contains the service measurement 6 count.
SM_CNT7	The sm_cnt7 field contains the service measurement 7 count.
SM_CNT8	The sm_cnt8 field contains the service measurement 8 count.
SM_CNT9	The sm_cnt9 field contains the service measurement 9 count.
SM_CNT10	Service Measurement Count 10
SM_CNT11	Service Measurement Count 11
SM_CNT12	Service Measurement Count 12
SM_CNT13	Service Measurement Count 13
SM_CNT14	Service Measurement Count 14
SM_CNT15	Service Measurement Count 15
SOURCE	The source field indicates the channel's name through which CIMs are collected. This field is validated against the name field of the source table.
ST	This field defines the valid service type. This field is case sensitive in display but search expressions are matched with no case sensitivity. The st field captures a code which shows the supplementary service invoked by the subscriber that receives an advise of charge. The code contains two components, the Supplementary Service Group and the Supplementary Service Code. The Supplementary Service Group is stored in the ssgrp field. The Supplementary Service Code is stored in the st field. This field is validated against the type field of the st table.
START_DATIME	The start_datime field contains the time when the call or session was initiated in, datetime format (down to the second).
TARGET_AP_NUM	The target_ap_num field indicates the Applications Processor to which the session balance is being transferred.
TARGET_OHM	The target_ohm field indicates the Overhead Manager to which the session balance is being transferred.
TC	The trouble category (tc) field is used to categorize FDCs, typically by error type (such as "nca") or by switch type (such as "5e").

Field	Description
TECH	The tech field shows the air side interface technology that was used on the call. Possible values are CDMA, CDMA2000, AMPS, TDMA, 2G, 3G, and Unknown.
TGN	The trunk group field (tgn) provides the trunk group number that was being used when the call irregularity was detected at the reporting office.
TP	The tp field identifies the traffic processor in the RNC. that generated this message.
TP_IPADDR	The tp_ipaddr field contains the IP Address of the Traffic Processor used for this session.
TRB	The trb (trouble name) field contains the CDR, message, log or report name, or the trouble code. This indicates the type of data that was used to generate the cfim record.
UATI	The uati field contains the universal access terminal identifier in a session setup attempt.
UATI_TIME	The uati_time field contains the timestamp indicating when the UATI assignment was acknowledged.
WEIGHT	The weight field provides the number of actual calls that this CDR represents, which can be used to provide meaningful reports in situations where some or all of the CDRs are sampled.

Sonus Mapping for CFIM

Purpose

The table below gives the mapping between the CFIM field and Sonus Attempt and Stop fields.

CFIM field	Attempt field	Stop field
announce_num	Directly from field 154	Directly from field 175
answer	-	From field 10 as conversion from ms to seconds
billdigits	Directly from field 25	Directly from field 28
billtype	null	Value “sonus”
busgrp	Directly from field 102	Directly from field 111
callid	Directly from field 72. This field is 32 bits in hex format, and is preceded by a “0x”, which is removed during population.	Directly from field 82. This field is 32 bits in hex format, and is preceded by a “0x”, which is removed during population.
caus	Directly from field 12	Directly from field 15
caus2	Directly from field 150	-
ccd	If nai field = 3 or 6 then ccd field is ferived form country table. Else if nai field equals 1, 2, 4 or 5 adn d field = “o” then is set to the ccd in the swarch record corresponding to the de, else if the nai field = 1, 2, 4 or 5 and d = “i”, then ccd is set to the ccd in the swarch record corresponding to the re, else is set to null.	
cic	Value in Type column from owner table.	Value in Type column from owner table.
city_npa	If nai field = 2, 3, 5 or 6 then city_npa field is derived from the city table, else if nai field equals 1 or 4 then the city_npa is set to the hnpa value from swarch table, else is set to null.	
cpbusgrp	Directly from field 101	Directly from field 110
cpcity_npa	If cpnai field = 2, 3, 5 or 6 then cpcity_npa field is derived from the city table, else if cpnai field equals 1 or 4 then the cpcity_npa is set to the hnpa value from swarch table, else is set to null.	
cpdigits	Directly from field 17	Directly from field 20
cplata	Directly from field 63	Directly from field 73
cpnai	Directly from field 43	Directly from field 50
cpnpt	Directly from field 99	Directly from field 108
csi	Directly from field 54	Directly from field 61
ct	The ct field is populated using ATTEMPT field 61 or STOP field 71, to match against the ctcode field of ctcode2ct table for records where ctname = “sonus”or ctname = “baf”.	
cust_tgn	Directly from field 168	Directly from field 194

CFIM field	Attempt field	Stop field
d	If field 57 is set to 1 or 4 then d field is set to “i”, else if is set to 2 then field d = “o”, else if is set to 0 or 3 and field 28 is not null field d = “o”, else if is set to 0 or 3 and field 28 is null field d = “i”.	If field 57 is set to 1 then d field is set to “i”, else if is set to 2 then field d = “o”, else if is set to 0 and field 28 is not null field d = “o”, else if is set to 0 and field 28 is null field d = “i”.
disc_loc	-	-
disc_loctr_ing	-	-
disc_loctr_egr	-	-
dpc	The dpc field is derived from the Remote Point Code part of field 34	The dpc field is derived from the Remote Point Code part of field 37
dsdigits	Directly from fields 18 and 19 if field 20 equals 1 and 22 equals 2 or if field 20 equals 2 and field 24 equals 2 Else If field 20 equals 2 and 22 equals 2 dsdigits is pupulated directly from field 23	Directly from fields 21and 2if field 23 equals 1 and 25 equals 2 or if field 23 equals 2 and field 27 equals 2 Else If field 23 equals 2 and 25 equals 2 dsdigits is pupulated directly from field 26
durat	-	From field 14 as conversion from ms to seconds.
egr_policing_ discpkts	-	Directly from field 174
egr_srtp_auth	-	First sub-field of field 181
egr_srtp_enc	-	Second sub-field of field 181
egr_srtcp_auth	-	Third sub-field of field 181
egr_srtcp_enc	-	Fourth sub-field of field 181
end_datime	Directly from fields 105 and 10	Directly from fields 11 and 12
end_setup	-	From field 9 as conversion from ms to seconds.
error_origin	If field 57 = 1 or 4 then the i field is set to “LLN” else if field 57 = 2 is set to “RLN” else if 0 or 3 is set to “TN”	If field 64 = 1 or 4 then the i field is set to “LLN” else if field 64 = 2 is set to “RLN” else if 0 or 3 is set to “TN”
fdc	The contents of field field 12 is matched against the acode field of acode2fdc, for records where the fname = “sonus”.	The contents of field field 15 is matched against the acode field of acode2fdc, for records where the fname = “sonus”.
fin_attempt	y if 146=1, "n" if 146=0, else null	-
i_ip	Directly from field 116	Directly from field 126
icodec	Directly from field 69	Directly from field 79
ict	Directly from field 86	Directly from field 95

CFIM field	Attempt field	Stop field
idelay	-	Directly from field 67
igtwy	From re field	From re field
ijitter	-	Directly from field 66
imaxout	-	Directly from field 152
ing_policing_ discpkts	-	Directly from field 173
ing_srtp_auth	-	First sub-field of 180
ing_srtp_enc	-	Second sub-field of 180
ing_srtcp_auth	-	Third sub-field of 180
ing_srtcp_enc	-	Fourth sub-field of 180
ipktloss	-	(field 65) / (field 42) *10,000
ircvd	-	Directly from field 42
isctn	Pupulated with Shelf:Slot:Port:DS0 part of field 32	Pupulated with Shelf:Slot:Port:DS0 part of field 35
isdn_acc_ind	-	-
isent	-	Directly from field 40
itgid	Directly from field 31	Directly from field 34
jip	Directly from field 37	Directly from field 44
lata	The lata field is derived from the latacode table, as a match.	
lnp	y if 22 and 24 equal 1, "n" otherwise.	y if 25 and 27 equal 1, "n" otherwise.
local_end	Directly from fields 10 and 105	Directly from fields 11 and 12
local_start	Directly from fields 6 and 7	Directly from fields 6 and 7
lrn	From 53 if 56 not null, otherwise from 18 and 19	From 60if 63 not null, otherwise from 21and 22
lrne	Directly from field 29	Directly from field 32
modem_tone_ sgnlvl	-	Directly from field 191
modem_tone_ type	-	Directly from field 190
nai	Directly from field 68, if field 68 is null, and field digits is not populated then nai is populated directly form field 144	Directly from field 78, if field 78 is null, and field digits is not populated then nai is populated directly form field 165
ncos	Directly from field 158	Directly from field 179

CFIM field	Attempt field	Stop field
netcall_ref_ci	-	-
netcall_ref_spc	-	-
next_cic	Directly from field 38	Directly from field 45
npt	Directly from field 145	Directly from field 166
ntwrk_id	Directly from field 156	Directly from field 177
occd	if cpnai = 3 or 6 then occd field is derived from the country table else if cpnai = 1, 2, 3 or 5 and d = “i” then occd field is set to the ccd in swarch table in from record corresponding to the de, else if cpnai = 1, 2, 3 or 5 and d = “o” then occd field is set to the ccd in swarch table in from record corresponding to the re, if cpnai is set to 7 then occd field is set to null.	
ocodec	Directly from field 70	Directly from field 80
odelay	-	Directly from field 151
oe	oe field is set to ne field of matching record from match of the jip field with the first 6 digits of the lrn field of lrn2ne.	
ogt	Directly from field 108	Directly from field 116
ogtwy	Determined from the first part of 28, if null then corresponding with clli from swarch table, else if field 28 is null the ogtwy field is set to the clli field of the swarch record where the ipaddress field matches the contents of field 35	determined from the first part of 31, if null then corresponding with clli from swarch table, else if field 31is null the ogtwy field is set to the clli field of the swarch record where the ipaddress field matches the contents of field 38
ojitter	-	Directly from field 150
oli	Directly from field 36	Directly from field 43
omaxout	-	Directly from field 153
opc	From field 32 as conversion from ms to seconds.	From field 35 as conversion from ms to seconds.
opktloss	-	(field 149) / (field 148 + field 149) *10,000
orcvd	-	Directly from field 148
orig_trk_type	Directly from field 147	Directly from field 167
osent	-	Directly from field 146
otgid	Directly from field 58, if null then directly from field 87	Directly from field 68, if null then directly from field 96
o_ip	Directly from field 30	Directly from field 33
partition_id	Directly from field 157	Directly from field 178
prev_cic	Directly from field 50	Directly from field 57
psn	Directly from field 60	Directly from field 70

CFIM field	Attempt field	Stop field
psx_cong	If field 129 = 0 then psx_cong is set to “clear”, if 1 then “low”, if 2 then “medium”, if 3 then high.	If field 139 = 0 then psx_cong is set to “clear”, if 1 then “low”, if 2 then “medium”, if 3 then high.
psx_id	psx_id field is set to psx_name from matching record from match of re and field 128 of ATTEMPT record as clli and psx_index of psxid2name table.	psx_id field is set to psx_name from matching record from match of re and field 138 of STOP record as clli and psx_index of psxid2name table.
psx_proctime	Directly from field 130	Directly from field 140
psx_test	Directly from field 170	Directly from field 196
re	Directly from field 2	Directly from field 2
rt	Directly from field 110	Directly from field 120
rttype	Directly from field 109	Directly from field 117
sig	If field d = “o” then field sig is populated from field 47 if d = “i” then from 46 field.	If field d = “o” then field sig is populated from field 54 if d = “i” then from 53 field.
sctn	Pupulated with Shelf:Slot:Port:DS0 part of field 34	Pupulated with Shelf:Slot:Port:DS0 part of 37
sdtt	Directly from field 14	Directly from field 17
st	The st field is populated using the following logic: 1. ATTEMPT field 80 or STOP field 89, Service Feature ID, is matched against the stcode2st table stcode field, with an stname of sonus. 2. ATTEMPT field 80 or STOP field 89, Service Feature ID, is matched against the stcode2st table stcode field, with an stname of baf. 3. If the previous step does not provide an st, ATTEMPT field 77 or STOP field 86, AMA Service Logic ID, is matched against the stcode2st table stcode field, with an stname of baf. 4. If the previous steps do not yield an st, then STOP field 43 (ATTEMPT field 36) is matched against the oline field of oline2st, and the st of the matching record is used for the st in cfim. 5. If the other fields do not yield an st value, then ATTEMPT field 13 or STOP field 16, Service Delivered, is matched against the stcode2st table stcode field, with an stname of sonus.	
start_datime	Directly from fields 6 and 7	Directly from fields 6 and 7
term_trk_type	Directly from field 148	Directly from field 168
tgn	Directly from field 87	Directly from field 96
tnsc	Directly from field 16	Directly from field 19
vpn_priv_ digits	Directly from field 151	Directly from field 170

CFIM field	Attempt field	Stop field
vpn_pub_ digits	Directly from field 152	Directly from field 171

Population of CFIM de Field

The de field is populated using the following logic for ATTEMPT records:

1. If field 57 (Disconnect Initiator) is set to 1 (Calling Party) or 4 (Calling Party Early), then:
   a. The de is determined from the de field of the univroute record where the tgid field of univroute matches the contents of field 31 (Ingress PSTN Trunk Name) and re matches re in univroute.
   b. If the previous step does not yield a match, then de is determined from the clli field of the swarch using Ingress Remote Gateway Address (ATTEMPT 116) where the ipaddress field of swarch matches the contents of field 116.
2. If field 57 (Disconnect Initiator) is set to 2 (Called Party), then:
   a. The de is determined from the de field of the univroute record where the tgid field of univroute matches the contents of field 58 (Egress Trunk Group Name) and re matches re in univroute.
   b. If the contents of field 58 do not match an re/tgid entry, or if field 58 is not populated, then de is determined from the de field of the univroute record where the tgn field of univroute matches the contents of field 87 (Egress Trunk Group ID) and re matches re in univroute. Any leading zeros in field 87 are removed before the match is attempted.
   c. If no match is found in the preceeding steps, then de is determined from the clli field of the swarch record where the ipaddress field of swarch matches the contents of ATTEMPT field 30 (Egress Remote Gateway Address).
3. If field 57 (Disconnect Initiator) is set to 0 (Internal) or 3 (Internal Early) and the content of field 28 (Route Selected) is not null, then the de is determined from the first part of field 28. This field is in the format of gateway_name:TGN. The de = the gateway_name portion of the route.

4. If field 57 (Disconnect Initiator) is set to 0 (Internal) or 3 (Internal Early) and the content of field 28 (Route Selected) is null, then the de is determined as follows:
   a. The de is determined from the de field of the univroute record where the tgid field of univroute matches the contents of field 31 (Ingress PSTN Trunk Name) and re matches re in univroute.
   b. If the previous step does not yield a match, then de is determined from the clli field of the swarch record and the Ingress Remote Gateway Address (ATTEMPT 116) , where the ipaddress field of swarch matches the contents of field 116.
5. If the previous steps fail due to insufficient data in the ATTEMPT record, then de is set to null. If the previous steps fail due to a match failure in univroute, then de is set to "?".

The de field is populated using the following logic for STOP records:

1. If the fdc field is set to "qos", then the de is determined from the first part of field 31. This field is in the format of gateway_name:TGN. The de = the gateway_name portion of the route.
2. If field 64 (Disconnect Initiator) is set to 1 (Calling Party), then:
   a. The de is determined from the de field of the univroute record where the tgid field of univroute matches the contents of field 34 (Ingress PSTN Trunk Name) and re matches re in univroute
   b. If the previous step does not yield a match, then de is determined from the clli field of the swarch using Ingress Remote Gateway Address (STOP 126) where the ipaddress field of swarch matches the contents of field 126.
3. If field 64 (Disconnect Initiator) is set to 2 (Called Party), then:
   a. The de is determined from the de field of the univroute record where the tgid field of univroute matches the contents of field 68 (Egress Trunk Group Name) and re matches re in univroute.
   b. If the contents of field 68 do not match an re/tgid entry, or if field 68 is not populated, then de is determined from the de field of the univroute record where the tgn field of univroute matches the contents of field 96 (Egress Trunk Group ID) and re matches re in univroute. Any leading zeros in field 96 are removed before the match is attempted.
   c. If no match is found in the preceeding steps, then de is determined from the clli field of the swarch record where the ipaddress field of swarch matches the contents of STOP field 33 (Egress Remote Gateway Address).
4. If field 64 (Disconnect Initiator) is set to 0 (Internal) and the content of field 31 (Route Selected) is not null, then the de is determined from the first part of field 31. This field is in the format of gateway_name:TGN. The de = the gateway_name portion of the route.

5. If field 64 (Disconnect Initiator) is set to 0 (Internal) and the content of field 31 (Route Selected) is null, then:
   a. The de is determined from the de field of the univroute record where the tgid field of univroute matches the contents of field 34 (Ingress PSTN Trunk Name) and re matches re in univroute.
   b. If no match is found in the previous step, then de is determined from the clli field of the swarch record where the ipaddress field of swarch matches the contents of field 126.
6. If the previous steps fail due to insufficient data in the STOP record, then de is set to null. If the previous steps fail due to a match failure in univroute, then de is set to “?”.

Appendix F: License Information for Open Source Software

Overview

Purpose

Network Trouble Patterning software incorporates a number of third-party open source software packages. This section provides the license and other legal information required by those software packages.

Contents

License Information

Apache Software

The Apache Software License, Version 2.0

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (http://www.apache.org/)." if and wherever such third-party acknowledgments normally appear.
4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ”AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SE VICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

OpenLDAP

The OpenLDAP Public License Version 2.3.19, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUND TION AND ITS CONTRIBUTORS ”AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF ME CHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

OpenSSL

Copyright (c) 1998-2005 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ”AS IS" AND ANY *EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ”AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Sun Microsystems, Inc.

Binary Code License Agreement for the JAVA 2 PLATFORM STANDARD EDITION DEVELOPMENT KIT 5.0

SUN MICROSYSTEMS, INC. ("SUN") IS WILLING TO LICENSE THE SOFTWARE IDENTIFIED BELOW TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT CAREFULLY. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACCEPT THE TERMS OF THE AGREEMENT. INDICATE ACCEPTANCE BY SELECTING THE "ACCEPT" BUTTON AT THE BOTTOM OF THE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS, SELECT THE "DECLINE" BUTTON AT THE BOTTOM OF THE AGREEMENT AND THE DOWNLOAD OR INSTALL PROCESS WILL NOT CONTINUE.

1. DEFINITIONS. "Software" means the identified above in binary form, any other machine readable materials (including, but not limited to, libraries, source files, header files, and data files), any updates or error corrections provided by Sun, and any user manuals, programming guides and other documentation provided to you by Sun under this Agreement. "Programs" mean Java applets and applications intended to run on the Java 2 Platform, Standard Edition (J2SETM platform) platform on Java-enabled general purpose desktop computers and servers.
2. LICENSE TO USE. Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of the Supplemental License Terms, Sun grants you a non-exclusive, non-transferable, limited license without license fees to reproduce and use internally Software complete and unmodified for the sole purpose of running Programs. Additional licenses for developers and/or publishers are granted in the Supplemental License Terms.
3. RESTRICTIONS. Software is confidential and copyrighted. Title to Software and all associated intellectual property rights is retained by Sun and/or its licensors. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. You acknowledge that Licensed Software is not designed or intended for use in the design, construction, operation or maintenance of any nuclear facility. Sun Microsystems, Inc. disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement. Additional restrictions for developers and/or publishers licenses are set forth in the Supplemental License Terms.
4. LIMITED WARRANTY. Sun warrants to you that for a period of ninety (90) days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided "AS IS". Your exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's

option to replace Software media or refund the fee paid for Software. Any implied warranties on the Software are limited to 90 days. Some states do not allow limitations on duration of an implied warranty, so the above may not apply to you. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.

5. DISCLAIMER OF WARRANTY. UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANT-ABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.
6. LIMITATION OF LIABILITY. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.
7. SOFTWARE FROM SOURCES OTHER THAN SUN. You acknowledge that, by your use of optional features of the Software and/or by requesting services that require use of the optional features of the Software, the Software may automatically download, install, and execute software applications from sources other than Sun ("Other Software"). Sun makes no representations of a relationship of any kind to licensors of Other Software. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE OTHER SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.
8. TERMINATION. This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Sun if you fail to comply with any provision of this Agreement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon Termination, you must destroy all copies of Software.

9. EXPORT REGULATIONS. All Software and technical data delivered under this Agreement are subject to US export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export, or import as may be required after delivery to you.
10. TRADEMARKS AND LOGOS. You acknowledge and agree as between you and Sun that Sun owns the SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET trademarks and all SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET-related trademarks, service marks, logos and other brand designations ("Sun Marks"), and you agree to comply with the Sun Trademark and Logo Usage Requirements currently located at http://www.sun.com/policies/trademarks. Any use you make of the Sun Marks inures to Sun's benefit.
11. U.S. GOVERNMENT RESTRICTED RIGHTS. If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).
12. GOVERNING LAW. Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.
13. SEVERABILITY. If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.
14. INTEGRATION. This Agreement is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

SUPPLEMENTAL LICENSE TERMS

These Supplemental License Terms add to or modify the terms of the Binary Code License Agreement. Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement . These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

1. Software Internal Use and Development License Grant. Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the Software complete and unmodified (unless otherwise specified in the applicable README file) for the purpose of designing, developing, and testing your Programs.
2. License to Distribute Software. Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified (unless otherwise specified in the applicable README file) and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software (unless otherwise specified in the applicable README file), (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that protects Sun's interests consistent with the terms contained in this Agreement, and (vi) you agree to defen d and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.
3. License to Distribute Redistributables. Subject to the terms and conditions of this Agreement, including but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute those files specifically identified as redistributable in the Software "README" file ("Redistributables") provided that: (i) you distribute the Redistributables complete and unmodified (unless otherwise specified in the applicable README file), and only bundled as part of Programs, (ii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README file), (iii) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (iv) you only distribute the Redistributables pursuant to a license agreement that protects Sun's interests consistent with the terms contained in the

Agreement, (v) y ou agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

4. Java Technology Restrictions. You may not modify the Java Platform Interface ("JPI", identified as classes contained within the "java" package or any subpackages of the "java" package), by creating additional classes within the JPI or otherwise causing the addition to or modification of the classes in the JPI. In the event that you create an additional class and associated API(s) which (i) extends the functionality of the Java platform, and (ii) is exposed to third party software developers for the purpose of developing additional software which invokes such additional API, you must promptly publish broadly an accurate specification for such API for free use by all developers. You may not create, or authorize your licensees to create, additional classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Sun in any naming convention designation.
5. Distribution by Publishers. This section pertains to your distribution of the Software with your printed book or magazine (as those terms are commonly used in the industry) relating to Java technology ("Publication"). Subject to and conditioned upon your compliance with the restrictions and obligations contained in the Agreement, in addition to the license granted in Paragraph 1 above, Sun hereby grants to you a non-exclusive, nontransferable limited right to reproduce complete and unmodified copies of the Software on electronic media (the "Media") for the sole purpose of inclusion and distribution with your Publication(s), subject to the following terms: (i) You may not distribute the Software on a stand-alone basis; it must be distributed with your Publication(s); (ii) You are responsible for downloading the Software from the applicable Sun web site; (iii) You must refer to the Software as JavaTM 2 Platform Standard Edition Development Kit 5.0; (iv) The Software must be reproduced in its entirety and without any modification whatsoever (including, without limitation, the Binary Code License and Supplemental License Terms accompanying the Software and proprietary rights notices contained in the Software); (v) The Media label shall include the following information: Copyright 2004, Sun Microsystems, Inc. All rights reserved. Use is subject to license terms. Sun, Sun Microsystems, the Sun logo, Solaris, Java, the Java Coffee Cup logo, J2SE , and all trademarks and logos based on Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. This information must be placed on the Media label in such a manner as to only apply to the Sun Software; (vi) You must clearly identify the Software as Sun's product on the Media holder or Media label, and you may not state or imply that Sun is responsible for any third-party software contained on the Media; (vii) You may not include any third party software on the Media which is intended to be a replacement or substitute for the Software; (viii) You shall indemnify Sun for all damages arising from your failure to comply with the requirements of this Agreement. In addition, you shall defend, at your expense, any and all claims brought against Sun by third parties, and shall pay all damages awarded by a court of competent

jurisdiction, or such settlement amount negotiated by you, arising out of or in connection with your use, reproduction or distribution of the Software and/or the Publication. Your obligation to provide indemnification under this section shall arise provided that Sun: (i) provides you prompt notice of the claim; (ii) gives you sole control of the defense and settlement of the claim; (iii) provides you, at your expense, with all available information, assistance and authority to defend; and (iv) has not compromised or settled such claim without your prior written consent; and (ix) You shall provide Sun with a written notice for each Publication; such notice shall include the following information: (1) title of Publication, (2) author(s), (3) date of Publication, and (4) ISBN or ISSN numbers. Such notice shall be sent to Sun Microsystems, Inc., 4150 Network Circle, M/S USCA12-110, Santa Clara, California 95054, U.S.A , Attention: Contracts Administration.

6. Source Code. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.
7. Third Party Code. Additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file. In addition to any terms and conditions of any third party opensource/freeware license identified in the THIRDPARTYLICENSEREADME.txt file, the disclaimer of warranty and limitation of liability provisions in paragraphs 5 and 6 of the Binary Code License Agreement shall apply to all Software in this distribution.

For inquiries please contact: Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. (LFI#141623/Form ID#011801)

Sun Microsystems, Inc.

Sun Microsystems, Inc. Binary Code License Agreement for the JAVA SE RUNTIME ENVIRONMENT (JRE) VERSION 6

SUN MICROSYSTEMS, INC. ("SUN") IS WILLING TO LICENSE THE SOFTWARE IDENTIFIED BELOW TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT CAREFULLY. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACCEPT THE TERMS OF THE AGREEMENT. INDICATE ACCEPTANCE BY SELECTING THE "ACCEPT" BUTTON AT THE BOTTOM OF THE AGREEMENT. IF YOU ARE NOT WILLING

TO BE BOUND BY ALL THE TERMS, SELECT THE "DECLINE" BUTTON AT THE BOTTOM OF THE AGREEMENT AND THE DOWNLOAD OR INSTALL PROCESS WILL NOT CONTINUE.

1. DEFINITIONS. "Software" means the identified above in binary form, any other machine readable materials (including, but not limited to, libraries, source files, header files, and data files), any updates or error corrections provided by Sun, and any user manuals, programming guides and other documentation provided to you by Sun under this Agreement. "Programs" mean Java applets and applications intended to run on the Java Platform, Standard Edition (Java SE) on Java-enabled general purpose desktop computers and servers.
2. LICENSE TO USE. Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of the Supplemental License Terms, Sun grants you a non-exclusive, non-transferable, limited license without license fees to reproduce and use internally Software complete and unmodified for the sole purpose of running Programs. Additional licenses for developers and/or publishers are granted in the Supplemental License Terms.
3. RESTRICTIONS. Software is confidential and copyrighted. Title to Software and all associated intellectual property rights is retained by Sun and/or its licensors. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. You acknowledge that Licensed Software is not designed or intended for use in the design, construction, operation or maintenance of any nuclear facility. Sun Microsystems, Inc. disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement. Additional restrictions for developers and/or publishers licenses are set forth in the Supplemental License Terms.
4. LIMITED WARRANTY. Sun warrants to you that for a period of ninety (90) days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided "AS IS". Your exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software. Any implied warranties on the Software are limited to 90 days. Some states do not allow limitations on duration of an implied warranty, so the above may not apply to you. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.
5. DISCLAIMER OF WARRANTY. UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANT-ABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

6. LIMITATION OF LIABILITY. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.
7. TERMINATION. This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Sun if you fail to comply with any provision of this Agreement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon Termination, you must destroy all copies of Software.
8. EXPORT REGULATIONS. All Software and technical data delivered under this Agreement are subject to US export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export, or import as may be required after delivery to you.
9. TRADEMARKS AND LOGOS. You acknowledge and agree as between you and Sun that Sun owns the SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET trademarks and all SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET-related trademarks, service marks, logos and other brand designations ("Sun Marks"), and you agree to comply with the Sun Trademark and Logo Usage Requirements currently located at http://www.sun.com/policies/trademarks. Any use you make of the Sun Marks inures to Sun's benefit.
10. U.S. GOVERNMENT RESTRICTED RIGHTS. If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).
11. GOVERNING LAW. Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

12. SEVERABILITY. If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.
13. INTEGRATION. This Agreement is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

SUPPLEMENTAL LICENSE TERMS

These Supplemental License Terms add to or modify the terms of the Binary Code License Agreement. Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement . These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

1. Software Internal Use and Development License Grant. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software "README" file incorporated herein by reference, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the Software complete and unmodified for the purpose of designing, developing, and testing your Programs.
2. License to Distribute Software. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software README file, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software, (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that protects Sun's interests consistent with the terms contained in this Agreement, and (vi) you agree to defend and indemnify Sun and its licensors from and
3. Java Technology Restrictions. You may not create, modify, or change the behavior of, or authorize your licensees to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Sun in any naming convention designation.

4. Source Code. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.
5. Third Party Code. Additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file. In addition to any terms and conditions of any third party opensource/freeware license identified in the THIRDPARTYLICENSEREADME.txt file, the disclaimer of warranty and limitation of liability provisions in paragraphs 5 and 6 of the Binary Code License Agreement shall apply to all Software in this distribution.
6. Termination for Infringement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right.
7. Installation and Auto-Update. The Software's installation and auto-update processes transmit a limited amount of data to Sun (or its service provider) about those specific processes to help Sun understand and optimize them. Sun does not associate the data with personally identifiable information. You can find more information about the data Sun collects at http://java.com/data/.

For inquiries please contact: Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A.

MOZILLA PUBLIC LICENSE

MOZILLA PUBLIC LICENSE Version 1.1

1. Definitions.

1.0.1. "Commercial Use" means distribution or otherwise making the Covered Code available to a third party.

1.1. "Contributor" means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code" means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable" means Covered Code in any form other than Source Code.

1.6. "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License" means this document.

1.8.1. "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

- A. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.
- B. Any new file that contains any part of the Original Code or previous Modifications.

1.10. "Original Code" means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

(b) under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

(c) the licenses granted in this Section 2.1(a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

(d) Notwithstanding Section 2.1(b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license

(a) under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

(c) the licenses granted in Sections 2.2(a) and 2.2(b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

(d) Notwithstanding Section 2.2(b) above, no patent license is granted: 1) for any code that Contributor has deleted from the 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

(a) Third Party Claims.

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs.

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the LEGAL file.

(c) Representations.

Contributor represents that, except as disclosed pursuant to Section 3.4(a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6. Versions of the License.

6.1. New Versions.

Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions.

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6.3. Derivative Works.

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7. DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED CODE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED CODE IS WITH YOU. SHOULD ANY COVERED CODE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

8. TERMINATION.

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declatory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

(a) such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

(b) any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent

infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10. U.S. GOVERNMENT END USERS.

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. MISCELLANEOUS.

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without

limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contracts License.

12. RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. MULTIPLE-LICENSED CODE.

Initial Developer may designate portions of the Covered Code as "Multiple-Licensed". "Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the NPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

EXHIBIT A -Mozilla Public License.

"The contents of this file are subject to the Mozilla Public License Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.mozilla.org/MPL/

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is _____.

The Initial Developer of the Original Code is _____.

Portions created by _____are Copyright (C) _____. All Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms of the license (the "[_____] License"), in which case the provisions of [_____] License are applicable instead of those above. If you wish to allow use of your version of this file only under the terms of the [_____] License and not to allow others to use your version of this file under the MPL, indicate your decision by deleting the provisions above and replace them with the notice and other provisions required by the [_____] License. If you do not delete the provisions above, a recipient may use your version of this file under either the MPL or the [_____] License."

[NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.]

Expat

Expat Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOL ERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Perl Artistic License

The Artistic License

Preamble

The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions:

- "Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.
- "Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder.
- "Copyright Holder" is whoever is named in the copyright or copyrights for the package.
- "You" is you, if you're thinking about copying or distributing this Package.

- "Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)
- "Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.

2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:

a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as ftp.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

b) use the modified Package only within your corporation or organization.

c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:

a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

b) accompany the distribution with the machine-readable source of the Package with your modifications.

c) accompany any non-standard executables with their corresponding Standard Version executables, giving the non-standard executables non-standard names, and clearly documenting the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Package as a product of your own.

6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whomever generated them, and may be sold commercially, and may be aggregated with this Package.

7. C or perl subroutines supplied by you and linked into this Package shall not be considered part of this Package.

8. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.

9. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The End

Heirloom mailx

Copyright (c) 1980, 1993 The Regents of the University of California. All rights reserved.

Copyright (c) 1996 Christos Zoulas. All rights reserved.

Copyright (c) 2000 Gunnar Ritter. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgements:
   - This product includes software developed by the University of California, Berkeley and its contributors.
   - This product includes software developed by Christos Zoulas.
   - This product includes software developed by Gunnar Ritter and his contributors.
4. Neither the name of the University nor the names of its contributors nor the name of Gunnar Ritter nor the names of his contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'', AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE DEVELOPERS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

For base64.c

Portions Copyright (c) 1991 Bell Communications Research, Inc. (Bellcore)

Permission to use, copy, modify, and distribute this material for any purpose and without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Bellcore not be used in advertising or publicity pertaining to this material without the specific, prior written permission of an authorized representative of Bellcore. BELLCORE MAKES NO REPRESENTATIONS ABOUT THE ACCURACY OR SUITABILITY OF THIS MATERIAL FOR ANY PURPOSE. IT IS PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES.

The Institute of Electrical and Electronics Engineers and The Open Group, have given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the 'nail' mail user agent, from IEEE Std 1003.1, 2003 Edition, Standard for Information Technology -- Portable Operating System Interface (POSIX), The Open Group Base Specifications Issue 6, Copyright (C) 2001-2003 by the Institute of Electrical and Electronics Engineers, Inc

and The Open Group. In the event of any discrepancy between these versions and the original IEEE and The Open Group Standard, the original IEEE and The Open Group Standard is the referee document.

The original Standard can be obtained online at http://www.opengroup.org/unix/online.html .

imap_gssapi.c:

imap_gssapi.c is partially derived from sample code in:

GSS-API Programming Guide

Part No: 816-1331-11

Sun Microsystems, Inc. 4150 Network Circle Santa Clara, CA 95054 U.S.A.

(c) 2002 Sun Microsystems

Copyright 1994 by OpenVision Technologies, Inc.

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of OpenVision not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. OpenVision makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

OPENVISION DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL OPENVISION BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

md5.h and md5.c are derived from RFC 1321:

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

hmac.c is derived from:

Network Working Group

Request for Comments: 2104

Category: Informational

H. Krawczyk

IBM

M. Bellare

UCSD

R. Canetti

IBM

February 1997

HMAC: Keyed-Hashing for Message Authentication

Status of This Memo

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Inno Setup License

Except where otherwise noted, all of the documentation and software included in the Inno Setup package is copyrighted by Jordan Russell.

Copyright (C) 1997-2007 Jordan Russell. All rights reserved.

This software is provided "as-is," without any express or implied warranty. In no event shall the author be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter and redistribute it, provided that the following conditions are met:

1. All redistributions of source code files must retain all copyright notices that are currently in place, and this list of conditions without modification.
2. All redistributions in binary form must retain all occurrences of the above copyright notice and web site addresses that are currently in place (for example, in the About boxes).

3. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software to distribute a product, an acknowledgment in the product documentation would be appreciated but is not required.
4. Modified versions in source or binary form must be plainly marked as such, and must not be misrepresented as being the original software.

Jordan Russell

jr-2007 AT jrsoftware.org

http://www.jrsoftware.org/

COPYRIGHT

Copyright (C) 1995-2009 Contributors

More detailed copyright information can be found in the individual source code files.

APPLICABLE LICENSES

---

* All NSIS source code, plug-ins, documentation, examples, header files and graphics, with the exception of the compression modules and where otherwise noted, are licensed under the zlib/libpng license.

* The zlib compression module for NSIS is licensed under the zlib/libpng license.

* The bzip2 compression module for NSIS is licensed under the bzip2 license.

* The LZMA compression module for NSIS is licensed under the Common Public License version 1.0.

ZLIB/LIBPNG LICENSE

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

BZIP2 LICENSE

This program, "bzip2" and associated library "libbzip2", are copyright (C) 1996-2000 Julian R Seward. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, Cambridge, UK. jseward@acm.org

COMMON PUBLIC LICENSE VERSION 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS "Contribution" means:

   a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

   b) in the case of each subsequent Contributor:

   i) changes to the Program, and

   ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

   a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

   b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

   c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

   d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

   A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

   a) it complies with the terms and conditions of this Agreement; and

   b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

   For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

   EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

   EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

   If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

   If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

   All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive. Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right

to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

SPECIAL EXCEPTION FOR LZMA COMPRESSION MODULE

Igor Pavlov and Amir Szekely, the authors of the LZMA compression module for NSIS, expressly permit you to statically or dynamically link your code (or bind by name) to the files from the LZMA compression module for NSIS without subjecting your linked code to the terms of the Common Public license version 1.0. Any modifications or additions to files from the LZMA compression module for NSIS, however, are subject to the terms of the Common Public License version 1.0.

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using this software ("Python") in source or binary form and its associated documentation.
2. ubject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010 Python Software Foundation; All Rights Reserved" are retained in Python alone or in any derivative version prepared by Licensee.
3. In the event Licensee prepares a derivative work that is based on or incorporates Python or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python.

4. PSF is making Python available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.
5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.
7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.
8. By copying, installing or otherwise using Python, Licensee agrees to be bound by the terms and conditions of this License Agreement.

Index