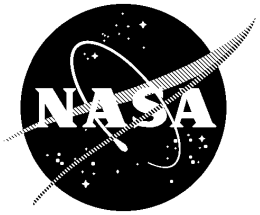
530-NCD-NCC98

MISSION OPERATIONS AND DATA SYSTEMS DIRECTORATE

Network Control Center (NCC) Central Delogger (NCD) Operations Concept

May 1997



National Aeronautics and Space Administration

Goddard Space Flight Center
Greenbelt, Maryland

Network Control Center (NCC) Central Delogger (NCD) Operations Concept

May 1997
Prepared Under Contract NAS5-31000

Prepared by:

Cindy Cacace Date
Booz·Allen & Hamilton Inc.

Approved by:

Roger Clason Date
NCC 98 Systems Engineer

Approved by:

Anthony Maione Date
NCC Project Manager

Goddard Space Flight Center
Greenbelt, Maryland

Preface

This document provides a concept of operations for the Network Control Center (NCC) Central Delogger (NCD) and its use in the NCC Data System (NCCDS). This document will address system interfaces with other NCCDS systems, define logging formats for other systems, and provide a foundation for design and implementation

Questions and proposed changes concerning this document shall be addressed to:

NCC 98 Systems Engineer
Code 530.5
Goddard Space Flight Center
Greenbelt, Maryland 20771

Abstract

This is the Network Control Center (NCC) Central Delogger (NCD) Operations Concept. This document will provide an overview of the function and layout of the NCD. The NCD will provide NCCDS users with a central, uniform, and efficient means to view specified data extracted from several log files.

Keyword: *NCD, NCC, NCC 98, Delogger*

Contents

Section 1. Introduction

1.1 Context

The Spaceflight Tracking and Data Network (STDN) is a complex communications network encompassing the Space Network (SN), Ground Network (GN), and all support facilities necessary to provide tracking, telemetry, and command (TT&C) support to customers. The STDN uses the geosynchronous Tracking and Data Relay Satellites (TDRSs), the ground terminals at the White Sands Complex (WSC), and the GN for supporting orbiting spacecraft.

The Network Control Center (NCC) is the STDN element responsible for overall, real-time coordination of network resources to satisfy the support requirements of all network customers. From a customer's perspective, the NCC is the operational interface for obtaining mission support. From a network element's perspective, the NCC is responsible for providing work schedules and coordinating problem resolution. NCC operations are accomplished through the NCC Data System (NCCDS) and ancillary systems.

Three segments of the 1998 version of the NCCDS, the Service Planning Segment Replacement (SPSR), the Communications and Control Segment (CCS), and the NCCDS Protocol Gateway (NPG), produce log files which record valuable information including message and process status information. In the course of development, testing, and operational use, NCC users will need to review the information stored in each system's log files. The NCC Central Delogger (NCD) will provide users with a central, uniform, and efficient means to view specified data extracted from the log files. NCD users will consist of anyone who can log on to the workstations and access the NCD and typically include operators, testers, and developers.

1.2 Purpose of the Document

During the course of NCC operations, it may be necessary to review data which has been logged by one or more of the SPSR, CCS, or NPG systems. The log files which are created contain a significant amount of information. The NCD will allow users to apply various filter criteria to extract the most relevant data and therefore decrease the amount of time examining log files.

This NCD operations concept will define NCD system functions and use in the NCC environment.

1.3 Document Organization

The remainder of this document is divided into three sections. Section 2 covers the programmatic considerations involved with the design of the NCD. These considerations include the goals and objectives of the NCD and NCC system constraints.

Section 3 introduces the NCD system environment with overviews on various components of the NCC Data System including the SPSR, CCS, and the NPG.

Section 4 discusses the NCD's system concepts which includes a description of how the NCD will operate. Section 4 explains how data will be delogged from log files and where these log files will be located with respect to the environment. Filter criteria used in the NCD delogging process will also be discussed.

Section 2. Programmatic Considerations

2.1 Goals and Objectives

The primary goal of the NCD is to provide an efficient method of locating and extracting relevant data from log files created by the SPSR, CCS, and NPG. At the present time, if an operator or tester requires specific data from a log file, one of the existing deloggers created specifically for each of the three systems must be utilized. This can cause confusion and increase the amount of time needed to access data. To solve this problem, these three systems will be required to adopt a common log file format allowing the NCD to delog files without translation and eliminate the individual delogging processes.

2.2 System Constraints

One of the major obstacles in designing the NCD is finding a location in the NCC where central delogging can take place. The central delogger should be located in an area where network traffic will be least affected by the delogging process. Another constraint to be dealt with is the fact that each of the three systems logging data has their own unique methods and data structures. This requires the adoption of a common log file format that will allow the NCD to delog the files without translation.

Section 3 System Environment

3.1 NCCDS System Overview

The following sections will discuss the three components of the NCCDS that are most relevant to the design of the NCD. These components are the SPSR, the CCS, and the NPG.

3.1.1 Service Planning Segment Replacement

The SPSR is maintained on a Hewlett Packard (HP) 9000 server. The SPSR receives and validates customer service requests, generates and maintains the schedule, and disseminates the schedule to the appropriate SN elements and customers.

The SPSR also receives acquisition data and maintains and disseminates acquisition data that the WSC uses for TDRS antenna pointing and Doppler shift prediction and compensation.

A key element of the SPSR is the database that maintains data relevant to TDRS services, customer spacecraft characteristics, SN customer characteristics, WSC resources, SN schedules, acquisition information, and the NCCDS operators. The database supports applications hosted on the SPSR and the CCS as well as other NCCDS segments.

3.1.2 Communications and Control Segment

The CCS contains three hardware and software components: a special-purpose computer—the Small Conversion Device (SCD), a general-purpose computer—a VAX 8550, and Operations Local Area Network (OpsLAN) connecting the SCD and VAX 8550. HP Workstations provide the display and interface to the VAX using Common Object Request Broker Architecture (CORBA). The CCS serves as the communications server that provides the interface between the NCCDS and external entities through Nascom.

The CCS also supports functions that are tightly coupled to high-speed message processing or are critical for real-time support of ongoing services such as service reconfiguration, and the receipt, validation, display, and dissemination of performance data. The CCS relies on the SPSR database for the active schedule and for user-specific control and configuration information.

3.1.3 NCCDS Protocol Gateway

The primary objective of the NPG is to provide translation of NCCDS high-speed external messages between the current Nascom 4800 Bit Block (BB) protocol and industry standard Internet protocols. This translation occurs at the transport layer and accounts for capabilities for

reliable end-to-end message communication. The NPG used in the NCC 98 final architecture is a Sun workstation.

3.2 NCD Environment

The hardware architecture for the NCD will be based on a HP platform. There will be one NCD server on a HP workstation. The NCD program will be accessible from any of the workstations through the toolbar.

There will be one common NCD environment. The NCD environment will provide all users the same capabilities regardless of data source. The only restriction to using the NCD will be the current workstation login restrictions. Anyone who can logon to the workstations can access the NCD. A workstation user will be able to review log file data through the NCD. A user will log on to the workstation, start the NCD program, and choose one of two data sources. One data source is log files Network File Server (NFS) mounted to the NCD server, allowing users to access files that still reside on each of the component systems via the NCD. At specified times, the log files resident on disk will be archived to tape by the Network and Systems Management (NSM) subsystem. Users may then download such archived files to the NCD server and delog from them.

All users will have the choice of whether to use the mounted files or download files from archived tapes. The operator should verify existing files so that downloading files do not overwrite these files. The files will be downloaded to a directory on the NCD server. The NCD will aid the user in viewing, sorting, and searching through the log data. Once the user has selected the files to view, the user may enter filter criteria and view the resultant data via display or report from the log files that are relevant to their analysis. Filter results may be saved to a file which can be accessed at a future time.

Figure 3-1 shows a high-level representation of the NCD environment.

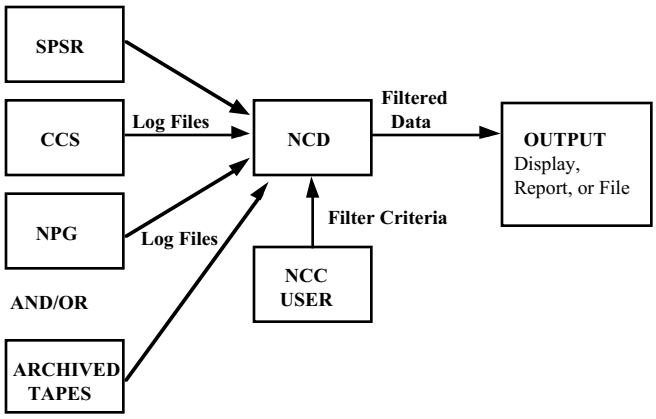


Figure 3-1 - NCD Environment

Section 4. System Concepts

4.1 Overview

The NCD (in the operations environment) will reside inside the NCCDS and be connected to all three systems by the OpsLAN. The systems participating in the logging and delogging process are highlighted in Figure 4-1.

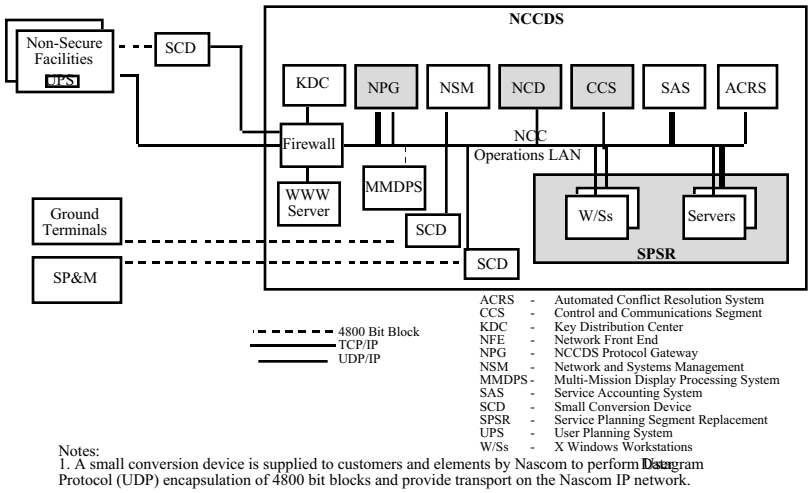


Figure 4-1 NCC 98 Architecture

Figure 4-1

4.2 NCD Interfaces

The next three sections discuss the interfaces between the NCD and the SPSR, CCS, and NPG with respect to the delogging process and include all files logged by each system. The NCD will retrieve the logged data needed from each system and will perform all necessary filtering and data reduction. The NCD will read 8mm tapes in the final system. Log data from the SPSR, CCS, and NPG will be delogged simultaneously and processed in ascending chronological order.

4.2.1 Interface Between NCD and SPSR

The interface between the NCD and the SPSR will provide the delogging capability for log files generated by the SPSR system. The NCD will be capable of extracting information from the SPSR log files resident on the SPSR server or those archived to tape. This data includes external Transmission Control Protocol/Internet Protocol (TCP/IP) messages received or transmitted and processed by the SPSR, certain process status information, and operator alerts and error messages generated by the SPSR application software.

4.2.2 Interface Between NCD and CCS

The interface between the NCD and the CCS will provide the delogging capability for log files generated by the CCS system. The NCD will be capable of extracting information from the CCS log files resident on the CCS disk or those archived to tape. This data includes external 4800BB messages received or transmitted and processed by the CCS, operator requests, data exchanges, and operator alerts and error messages generated by CCS application software.

4.2.3 Interface Between NCD and NPG

The interface between the NCD and the NPG will provide the delogging capability for log files generated by the NPG system. The NCD will be capable of extracting information from the NPG log files resident on the NPG system or those archived to tape. This data includes external TCP/IP, User Datagram Protocol/Internet Protocol (UDP/IP), and 4800BB formatted messages received or transmitted and processed by the NPG, certain process status information, and operator alerts and error messages generated by NPG application software.

4.3 Log File Names

Data will be logged by each of the three systems using a common logging procedure and file format. The log files must have accurate time-stamp file names to precipitate the delogging process. The file name format is as follows:

YYYYDDDHHMMSSMMM.SYS

Where YYYY represents the year the file was created, DDD represents the day of the year, HH represents the hour, MM represents the minute, SS represents the second, and MMM represents a millisecond. The filename extension will represent the system from which the log file originated. A file extension of “SPS” will represent a SPSR log file, “CCS” will represent a CCS log file, and “NPG” will represent an NPG log file. The extensions will eliminate the possibility of two different files having identical file names.

4.4 Data Logged

There are several types of data that may be logged by one or all of the three systems. The data includes external messages, error messages and alerts, operator requests and data exchanges, and process information. The following sections describe data logging specifications as found in the NCCDS System Requirements 1998. The NCD design phase will identify all data that is logged regardless of whether or not it was specified in the NCCDS requirements. During the NCD design phase, all data to be logged will be identified by the SRD and SPSR, CCS, and NPG developers.

4.4.1 External Messages

The NCCDS logs all TCP/IP, UDP/IP, and 4800BB messages received from or transmitted to external entities, except for those incoming messages that fail communication protocol checks.

4.4.2 Error Messages and Alerts

The NCCDS logs all alerts and error messages to NCC operators and all inputs by NCC operators, including free-text comments and entries to acknowledge action alerts.

4.4.3 Operator Requests and Data Exchanges

The NCCDS logs all operator requests and data exchanges resulting from these requests including the data interface between CCS and SPSR. The NCD log files used from SPSR will not include any database updates between the SPSR and the database. The log files will include messages but not actual database commands.

4.4.4 Process Information

The NCCDS logs all process information including process start time and end time. For example, the time that an external entity establishes a connection with the NPG and the time that the connection is broken will be logged.

4.5 Log File Format

With the ability to use Internet protocols to transfer messages, it becomes necessary to define log header formats to account for both 4800BBs and Internet protocol messages. Appendix A contains log file format information for SPSR, CCS, and NPG.

4.6 Data Retrieval

4.6.1 Filter Criteria

The NCD will utilize several filter criteria to aid in searching through the log files. Retrieval from log file entries will be dependent on entries in the log file matching a specified input value, which may represent one value within a list of specified values. The specified value may also represent one value within a specified range of values for each member of any specified subset of the filter criteria. The filter criteria for 4800BB and Internet protocol messages consists of the following characteristics: log time, source, destination, message type, message type and class, SIC, SUPIDEN, TDRS (TDRS ID and TDRS Name), TDRSS service, SN element, any data field, operator console, and operator position. Filtering by system or log source will also be available (e.g., CCS, SPS, NPG). Filter criteria may be saved to file for future and repeated use.

4.6.2 Output

The NCD will provide the operator with the capability to designate the physical form of output. From the logged data, the NCD will be capable of generating the following:

〈 Hardcopy output

〈 NCC workstation displays

〈 File output to be used to generate hardcopy output at a later time.

4.7 Data Retention

The logged data gathered in the operations environment will be archived by NSM to log tapes and retained for a minimum of 90 days following the end of the applicable operational day as stated in the NCCDS System Requirements 1998 (Section 8.2.5).

4.8 Use of the NCD

An NCD will reside on each of the NSM backup servers in the OCR, ANCC, and DT&T. In the event that NSM needs to run from the backup server, the NCD may be used only in the DT&T. There will be events, such as change or loss of an event or data, that warrant the use of a central delog. To analyze the cause, a user will delog the log files using the NCD. The user first needs to determine whether the log data is resident on the individual systems or backed up by NSM. If the data does not reside on the systems, the user will request the NSM operator to locate the tape containing the data and restore from backup using Omniback. The user will then filter and analyze the data using the NCD.

Appendix A. NCD Log Header

Introduction

This appendix outlines the logging information associated with the NCD. Three areas are addressed: the location of the log files, the naming convention of the log files, and the log file format.

Location of Log Files

Each system will have a specified directory where all log files will reside. The location of the log files shall be determined by each individual system and shall remain constant throughout operational use. The log files will remain in these directories until they are archived to tape via the NSM tools.

Log File Naming Conventions

Each log file name will follow a standard naming convention. The log file name will be the Universal Time Coordinated (UTC) when the log file was created. The log file name shall adhere to the "YYYYDDDHHMMSSMMM.SYS" format where:

YYYY	is	year	[1997, 1998, 1999, 2000, 2001, ...]
DDD	is	day of year	[001 – 366]
HH	is	hour	[00 - 23]
MM	is	minute	[00 - 59]
SS	is	second	[00 - 59]
MMM	is	millisecond	[000 – 999]
SYS	is	system	[SPS, CCS, or NPG]

Log File Format

The log file format applies to data logged by the SPSR, the CCS, and the NPG. A log file consists of a continuous series of log file entries. The log file entries are in ascending chronological order according to the UTC timestamp associated with each entry. There is no special character or termination method used to separate the log file entries. Each log file entry consists of two parts: the log header and the data itself. This section addresses the log header part only. The data logged

is addressed in the overall Interface Control Documents (ICDs) and individual system documentation. [Note: for 4800BB, bytes 1 - 596 are logged as the data, whereas bytes 597 - 600 [the Polynomial Error Protection (PEP) bytes] are logged in the log header.]

Tables A-1 through A-4 outline the fields with their valid values for the log header. Table A-5 shows sample log file formats for each system. Table A-6 shows the 'C' language log header structure.

Table A-1
Log Header Fields

Field Name		Valid Values	Applicable to 4800BB	Applicable to TCP/IP	Applicable to Others
year	4 characters	ASCII representation of the year [i.e., 1997, 1998, 1999, 2000, 2001, …]	yes	yes	yes
day	3 characters	ASCII representation of the day of year [001 - 366]	yes	yes	yes
hour	2 characters	ASCII representation of the hour [00 - 23]	yes	yes	yes
minute	2 characters	ASCII representation of the minute [00 - 59]	yes	yes	yes
second	2 characters	ASCII representation of the second [00 - 59]	yes	yes	yes
millisecond	3 characters	ASCII representation of the millisecond [000 - 999]	yes	yes	yes
proc_id	4 characters	see Process ID Table	yes	yes	yes
length	short (2 bytes)	length of data logged, not including the header	yes	yes	yes
log_source	1 character	S = SPSR C = CCS N = NPG	yes	yes	yes
io_flag	1 character	see IO Flag Table	yes	yes	yes
pep	4 characters	Bytes 597 - 600 of 4800BB	yes	yes	yes
ip_address	16 characters	see IP Address Table	no	yes	yes, when applicable
protocol_port	int (4 bytes)	as specified in NCCDS/MOC ICD	no	yes	yes, when applicable

Note: "Others" includes alerts, error messages, process information, operator requests, and data exchanges that result from operator requests.
All bytes of non-applicable fields should be filled with the Null character.

Table A-2
Process ID Table

System	Process ID	Type of Data Logged
SPSR	OPEV	operator events
SPSR	EXMG	external TCP/IP messages
SPSR	ALRT	error messages and alerts
SPSR	PINF	process information
CCS	FELC	UDPR receive data from NPG and UDPT send data to NPG (4800BB format)
CCS	NMSV	UPD select/deselect GUI server requests
CCS	EMSV	GCM GUI server requests
CCS	ASSV	review events GUI server requests
CCS	CTSV	CTB GUI server requests
CCS	SSSV	site status GUI server requests
CCS	ODMC	ODM GUI server requests
CCS	DBSF	static data exchanges
CCS	DBEF	event data exchanges
NPG	EXBK	external 4800BB blocks
NPG	EXMG	external TCP/IP messages
NPG	ALRT	error messages and alerts
NPG	PINF	process information

Table A-3
IO Flag Table

System	IO Flag	Data Logged
SPSR	I	TCP/IP messages received
SPSR	O	TCP/IP messages transmitted
SPSR	O	error messages and alerts
SPSR	O	process information
CCS	I	4800BB received
CCS	O	4800BB transmitted
CCS	I	operator requests
CCS	O	data exchanges as result of operator requests
CCS	O	error messages and alerts
NPG	I	4800BB and TCP/IP messages received
NPG	O	4800BB and TCP/IP messages transmitted
NPG	O	error messages and alerts
NPG	O	process information

Table A-4
IP Address Table

System	Data Logged	IP Address
SPSR	TCP/IP messages received	IP address of the transmitter of the message
SPSR	TCP/IP messages transmitted	IP address of the receiver of the message
SPSR	error messages and alerts	N/A
SPSR	process information	N/A
CCS	4800BB received	N/A
CCS	4800BB transmitted	N/A
CCS	operator requests	N/A
CCS	data exchanges as result of operator requests	N/A
CCS	error messages and alerts	N/A
NPG	4800BB received	N/A
NPG	4800BB transmitted	N/A
NPG	TCP/IP messages received	IP address of the transmitter of the message
NPG	TCP/IP messages transmitted	IP address of the receiver of the message
NPG	error messages and alerts	IP address of the receiver of the error message or alert (or N/A if not sent to workstation)
NPG	process information	N/A

Table A-5
Sample Log File Formats

Sample SPSR Log File Format	Sample CCS Log File Format	Sample NPG Log File Format
Log Header	Log Header	Log Header
Process Information	4800BB	4800BB
Log Header	Log Header	Log Header
IP Message	4800BB	IP Message
Log Header	Log Header	Log Header
Error/Alert	Server Request	Error/Alert
. . .	. . .	. . .
Log Header	Log Header	Log Header
IP Message	Data Exchange	IP Message
Log Header	Log Header	Log Header
Operator Event	Error/Alert	Process Information

Table A-6
'C' Language Log Header Structure

```
typedef  struct  log_hdr
{
        char    year[4];
        char    day[3];
        char    hour[2];
        char    minute[2];
        char    second[2];
        char    millisecond[3];
        char    proc_id[4];
        short   length;
        char    log_source;
        char    io_flag;
        char    pep[4];
        char    ip_address[16];
        int     protocol_port;
}  LOG_HDR;
```

Acronyms and Abbreviations

ACRS	Automated Conflict Resolution System
ANCC	Auxiliary Network Control Center
BB	Bit Block
CCS	Communications and Control Segment
CORBA	Common Object Request Broker Architecture
DT&T	Development, Test & Training
GN	Ground Network
HP	Hewlett Packard
LAN	Local Area Network
MMDPS	MultiMission Display Processing System
Nascom	NASA Communications
NCC	Network Control Center
NCD	NCC Central Delogger
NCCDS	NCC Data System
NFS	Network File Server
NPG	NCCDS Protocol Gateway
NSM	Network and Systems Management
OCR	Operations Control Room
OpsLAN	Operations LAN
PEP	Polynomial Error Protection
SAS	Service Accounting Segment
SCD	Small Conversion Device

SN	Space Network
SPSR	Service Planning Segment Replacement
STDN	Spaceflight Tracking and Data Network
TCP/IP	Transmission Control Protocol/Internet Protocol
TDRS	Tracking and Data Relay Satellite
TDRSS	Tracking and Data Relay Satellite System
TT&C	Telemetry, Tracking and Command
UDP/IP	User Datagram Protocol/Internet Protocol
UPS	User Planning System
UTC	Universal Time Coordinated
WSC	White Sands Complex
W/S	X Windows Workstation