

CA MICS® Resource Management

Network Analyzer Option Guide

Release 12.9



This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time. This Documentation is proprietary information of CA and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2014 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At <http://ca.com/support>, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at <http://ca.com/docs>.

Contents

Chapter 1: OVERVIEW	11
1.1 Primary Areas of Application.....	13
1.2 Major Features	14
1.3 Reporting and Inquiry Facilities.....	17
1.4 Files Overview	33
1.5 Product Prerequisites.....	35
1.6 Benefits	36
 Chapter 2: USAGE CONSIDERATIONS	 39
2.1 Introduction to the Use of Network Data	40
2.2 General Analysis Considerations	42
2.2.1 Pre-SNA Communications	43
2.2.2 SNA Overview.....	46
2.2.3 Comparison of SNA and the OSI Model	79
2.2.4 TCP/IP Overview.....	81
2.3 Use Within the Information Structure	82
2.3.1 Introduction to the Information Structure.....	83
2.3.2 Index into the Information Structure	85
2.3.3 Service Level Analysis.....	87
2.3.4 Installation Environment Analysis.....	110
2.4 Specialized Analysis	146
2.5 Data Manipulation Guidelines.....	153
2.6 Multiple Session Manager Considerations.....	156
 Chapter 3: TABULAR REPORTS, GRAPHS, AND MICF INQUIRIES	 161
3.1 Tabular Reports	162
3.1.1 Producing Tabular Reports.....	163
3.1.2 Tabular Report Formats	170
3.1.3 Tabular Report Descriptions	171
3.2 Sample Graphics	283
3.2.1 How to Produce Sample Graphics.....	284
3.2.2 Sample Graphics Descriptions.....	291
3.3 MICF Inquiries	304
3.3.1 MICF Inquiry Descriptions	305
3.3.2 How to Modify Standard MICF Inquiries.....	480

Chapter 4: EXCEPTION REPORTING

493

4.1 Philosophy and Requirements	495
4.2 Exception Processing	496
4.3 Using the Exception Reports for Problem Analysis	497
4.4 Identification and Qualification.....	498
4.4.1 SNA Exception Number Assignment	499
4.4.2 Severity Level Definition	500
4.4.3 Management Area Definition.....	501
4.5 CA MICS Network Standard Exceptions List	502
4.6 Detail Exception Descriptions.....	504

Chapter 5: DATABASE FILES

637

5.1 Data Element Naming Conventions	638
5.2 SNT Information Area.....	639
5.2.1 NCP Link File (SNTNCL)	640
5.2.2 Network Components Activity File (SNTCAF).....	649
5.2.3 NCP Activity File (SNTNAF)	656
5.2.4 Network Incident File (SNTNIN)	665
5.2.5 NPM User Activity File (SNTPSU).....	672
5.2.6 NPM System (PLU) Activity File (SNTPSY)	682
5.2.7 NPM Link Activity File (SNTNPL).....	692
5.2.8 NPDA Event File (SNTNEF).....	703
5.2.9 NPDA Statistical File (SNTNSF)	710
5.2.10 NPDA LAN File (SNTLNF).....	716
5.2.11 NPDA Generic Alert File (SNTGAF)	724
5.2.12 NLDM Service File (SNTNSV)	729
5.2.13 CA NetSpy Application (PLU) File (SNTNSP)	737
5.2.14 CA NetSpy Terminal (SLU) File (SNTNSS).....	744
5.2.15 CA NetSpy Virtual Route Activity File (SNTNVR)	753
5.2.16 NCP Network Accounting File (SNTNAC).....	761
5.2.17 NCP Line Processor Activity File (SNTNLP)	771
5.2.18 Telnet Server Entry File (SNTNTS)	779
5.2.19 Stack Entry File (SNTTCS)	787
5.2.20 VTAM Buffer Pool Data File (SNTVBS).....	794
5.2.21 VTAM CSM Data File (SNTVCS).....	801
5.2.22 VTAM Global Data File (SNTVGB).....	809
5.3 NVS Information Area	816
5.3.1 NLDM System (PLU) Activity File (NVSLSY)	817
5.3.2 NLDM Session Accounting File (NVSNSA)	826
5.3.3 NLDM Session Connectivity File (NVSNSC).....	834
5.3.4 NLDM Link Activity File (NVSNLL).....	842

5.3.5 NLDL Route File (NVS RTE)	850
5.3.6 NLDL Response Time File (NVS RTM)	858
5.3.7 NLDL VTAM BIND Failure File (NVS VBF)	866
5.4 TCP Information Area	873
5.4.1 Telnet Server File (TCPSTN)	873
5.4.2 Telnet Client File (TCPCTN)	881
5.4.3 FTP Server File (TCPFSF)	888
5.4.4 FTP Client File (TCPFCF)	896
5.4.5 API Calls for Sockets File (TCPAPI)	904
5.4.6 FTP Login Failure File (TCPFLF)	911
5.4.7 IP Statistics File (TCPIPX)	917
5.4.8 ICMP Statistics File (TCPICX)	925
5.4.9 TCP Statistics File (TCPTCI)	933
5.4.10 UDP Statistics File (TCPUDI)	941
5.4.11 Storage Statistics File (TCPSTG)	948
5.4.12 Interface Statistics File (TCPIFS)	955

Chapter 6: DATA SOURCES 963

6.1 Data Sources Overview	964
6.1.1 NetView Performance Monitor (NPM)	965
6.1.2 NetView Session Monitor (NLDL)	973
6.1.3 NetView Hardware Monitor/NPDA	977
6.1.4 CA NetSpy	978
6.1.5 CA NetMaster Network Tracking System (NTS)	997
6.1.6 CA NetMaster Network Error Warning System (NEWS)	999
6.1.7 CA NetMaster for TCP/IP	1000
6.1.8 IBM TCP/IP (TCP)	1001
6.2 Processing Network Monitor Data From VM Hosts	1002
6.2.1 Tivoli NetView Performance Monitor (NPM)	1003
6.2.2 CA NetSpy	1007
6.2.3 Tivoli NetView	1016
6.2.4 CA NetMaster	1020
6.2.5 CA MICS Requirements for Data Input	1024
6.3 Correlating Data Sources	1025
6.3.1 Correlating Data Sources to Reports	1026
6.3.2 Relationship of Data Sources to CA MICS Files	1029
6.3.3 Establishing a Network Identifier (NETWRKID)	1041
6.3.4 Defining Time Zone Offsets	1042
6.3.5 Establishing TP Circuit Identifier (LNKTPCID)	1043
6.3.6 Ensuring All Required Input Data Is Present	1044
6.3.7 CA NetSpy and IBM TCP/IP SMF Data	1045

6.3.8 Establishing a Single Value for PLU (SNTPLURT)	1046
6.3.9 Important Usage Notes for the NLL and LSY Files	1048
6.3.10 Determining Number of Route Element/TG Names	1050
6.3.11 CA NetSpy Data Considerations	1051
6.4 Exceptions and NPM Network Parameters	1056
6.4.1 Correlating Data Sources to Reports	1057
6.4.2 NPM Network Parameters Required for Exceptions	1059
6.4.3 Creating Performance Classes for Reporting	1060
6.4.4 Adding Tabular Reports to the DAILY Job	1061
6.5 NPA to File Conversion Utility	1061
6.6 Basic Network Accounting	1062
6.6.1 Accounting Information Sources	1064
6.6.2 Identification of Sessions for Differential Billing	1066
6.7 Identifying Local Vs. Remote Sessions (fflDEV)	1070
6.8 Multiple Session Manager Considerations	1071
6.9 Processing Network Monitor Data From VM Hosts	1075
6.10 CA MICS and CA SMF Director Interface	1076

Chapter 7: PARAMETERS **1079**

7.1 Environmental Considerations	1080
7.2 Complex-level Parameters	1081
7.2.1 Analyzer Definition Statements (SNTGENIN)	1082
7.2.2 Account Code Definition (SNTACCT)	1084
7.2.3 Account Code Exit Routine Definition (SNTACRT)	1092
7.3 Unit-level Parameters	1097
7.3.1 Processing Options (SNTOPS)	1099
7.3.2 INPUTRDR and INPUTSNT PARMS Members	1183
7.3.3 JCL Option Definitions (JCLDEF)	1189
7.3.4 Network Identifier Exit (SNTNIDRT)	1190
7.3.5 Link TP Circuit ID Exit (SNTCIDRT)	1192
7.3.6 Network Service Group Definition (NETGROUP)	1195
7.3.7 Network Service Group Exit Routine (NETGPRT)	1200
7.3.8 Network Application Table (NETAPPL)	1202
7.3.9 PLU Identification Routine (SNTPLURT)	1204
7.3.10 Database Space Modeling (DBMODEL)	1209

Chapter 8: MANAGEMENT SUPPORT APPLICATION INTERFACES **1213**

8.1 CA MICS Accounting and Chargeback Interface	1213
8.1.1 Chargeback Considerations	1214
8.1.2 Billable Elements	1217
8.1.3 Network Accounting Considerations	1217

8.2 CA MICS Capacity Planner Interface.....	1220

Chapter 9: PROCESSING	1221

9.1 Processing Considerations.....	1222
9.2 DAILY Update Processing Flow	1224

Chapter 10: MODIFICATION	1239

10.1 Available User Exits	1242
10.2 Exit Routine Considerations	1245
10.3 Input Exits.....	1246
10.4 Output Exits.....	1252
10.5 Implement Incremental Update.....	1287

Appendix A: Messages	1291

Messages.....	1291

Appendix B: DATA DICTIONARY	1363

Chapter 1: OVERVIEW

The CA MICS Network Analyzer processes data from operational and network management tools that operate in IBM's System Network Architecture (SNA). Additionally, it processes data generated by IBM TCP/IP for z/OS stacks. CA MICS automatically integrates Network Analyzer information with other information that it maintains. This is possible because the CA MICS Network Analyzer stores information in a format that is common to all CA MICS products.

Because failure or inadequate performance of data communications facilities can adversely affect business operations, today's large computer installations require sophisticated data communications capabilities such as those provided by IBM TCP/IP and SNA. Products that support IBM TCP/IP and SNA permit you to manage day-to-day network operations and to respond to user problems, complaints, and questions, but they do not provide an effective way to address long-term management control issues.

The CA MICS Network Analyzer lets you manage your communications networks systematically. It provides a single overall network perspective by offering easy access to large amounts of data taken from many sources and displaying it in a meaningful way.

The CA MICS Network Analyzer is one of the many Data Integration Applications of CA MICS. Like the other Data Integration Applications, it processes raw data for analyzing and managing specific technologies.

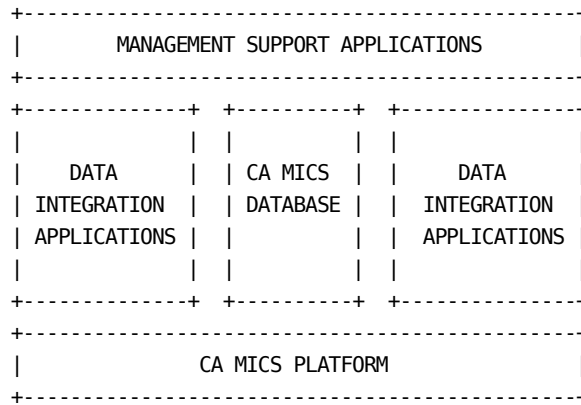


Figure 1-1. CA MICS

CA MICS is a comprehensive, flexible application system that applies standard management practices to the I/S organization. Designed with a formal architecture, CA MICS uses integrated applications similar to the integrated financial applications that are now indispensable to corporate financial management.

This section contains the following topics:

- [1.1 Primary Areas of Application](#) (see page 13)
- [1.2 Major Features](#) (see page 14)
- [1.3 Reporting and Inquiry Facilities](#) (see page 17)
- [1.4 Files Overview](#) (see page 33)
- [1.5 Product Prerequisites](#) (see page 35)
- [1.6 Benefits](#) (see page 36)

1.1 Primary Areas of Application

The CA MICS Network Analyzer provides analysis and reporting capabilities that help you to manage complex IBM TCP/IP and SNA networks in the following areas:

- o Network Service - The CA MICS Network Analyzer provides network, host, and total response time information, including average, peak, and response distribution percentages to allow you to evaluate actual service against established service levels.
- o Network Reliability - The CA MICS Network Analyzer information concerning temporary and permanent errors in the network's logical and physical components allows you to identify patterns and trends so that you can focus on the specific components that are degrading network reliability.
- o Network Performance - As network resources become overloaded, network performance deteriorates. CA MICS Network Analyzer information allows you to anticipate, identify, and correct the conditions that can cause this deterioration.
- o Network Activity - The CA MICS Network Analyzer provides information about network activity patterns and workloads that allows you to track and understand current activity and plan for future requirements.
- o Network Charges - The CA MICS Network Analyzer provides information (including connect time and characters transmitted) suitable for billing network resource users. The integration of CA MICS Network Analyzer data and CA MICS Accounting and Chargeback permits you to perform accounting functions using SNA network information from CA NetSpy Network Performance, the NetView Performance Monitor (NPM), the NetView Session Monitor (NLDM), and CA NetMaster Network Performance.

In addition, the CA MICS Network Analyzer provides TCP/IP analysis and reporting capabilities that help you to manage your TCP/IP activity across an enterprise wide network.

1.2 Major Features

The major features of CA MICS Network Analyzer can be grouped into four categories:

- o Report facilities
- o Use of IBM TCP/IP for z/OS and SNA network data
- o General product flexibility
- o Interface capabilities

Report Facilities

The CA MICS Network Analyzer provides the following reports:

- o Exception Reports allow you to define, capture, and report on network conditions that deviate from the expected norm.
- o Standard Analysis Reports include:
 - Service Reports that quantify response data and allow you to analyze the service being provided to end users.
 - Workload Reports that display workload and utilization levels for network nodes, including physical and logical network resources.
 - Data Collection Reports that provide an overview of the response time, service, and network load associated with end users.
 - Network Incident Reports that provide network error information by resource and incident type.
- o Graphics Analysis Reports help you to effectively communicate how well your network is serving the end user. Available through the CA MICS Information Center Facility (MICF), these inquiries include:
 - Service Level Graphic Inquiries that display response information from NPM, CA NetSpy, NetView, and CA NetMaster data sources.
 - Resource Utilization and Consumption Inquiries that display information about network component

utilization.

- Reliability Inquiries that show error counts or rates for those system resources that are the most critical and that fail most often.

Use of IBM TCP/IP for z/OS and SNA Network Data

An important feature of the CA MICS Network Analyzer is its comprehensive handling of SNA data.

- o It provides a common database to support a variety of information across many SNA network monitor data sources as well as data source from IBM TCP/IP for z/OS.
- o It integrates network monitor data with application monitor data.
- o It combines monitor-generated exceptions from the NPM Network Subsystem with user-defined exceptions from the NPM Session Subsystem, NetView Session Monitor, NetView Hardware Monitor, CA NetSpy, and CA NetMaster.
- o It excludes erroneous and redundant monitor data from the CA MICS database, increasing both data reliability and usability.
- o It eliminates duplicate data for cross-domain sessions when NetView is running on multiple hosts.

General Product Flexibility

The CA MICS Network Analyzer offers a number of flexibility features:

- o Information in a form suitable for basic network accounting, and the necessary structure to support chargeback through CA MICS Accounting and Chargeback.
- o Usage guidelines for analyzing and reporting network management information.

- o A Data Dictionary that describes the information found in the CA MICS Network Analyzer database.
- o Time zone translation to simplify combining data from geographically dispersed network nodes into the same CA MICS files.
- o A wide range of standard exits that allow you to examine, alter, extract, or delete data as required.

Interface Capabilities

The CA MICS Network Analyzer integrates the data collected by IBM TCP/IP for z/OS, NPM (NetView Performance Monitor), NetView Session Monitor/NLDM, CA NetSpy, and CA NetMaster into the CA MICS database. This process creates the CA MICS Network, the NetView Session, and TCP/IP Information Areas, all of which interface with the following CA MICS products:

- o CA MICS Accounting and Chargeback - The CA MICS Network Analyzer provides network data to CA MICS Accounting and Chargeback that supports accounting for consumed resources through a variety of resource utilization measures (for example, characters transmitted, session connect time, and so forth).
- o CA MICS Capacity Planner - The CA MICS Network Analyzer maintains a database of detailed and summarized network data that the CA MICS Capacity Planner can use to make growth/trend projections at the system, organizational, application, and end-user levels.

1.3 Reporting and Inquiry Facilities

CA MICS Network Analyzer Option standard reports and online inquiries provide concise, comprehensive information to help you manage your SNA network resources.

CA MICS Network Analyzer Option provides standard analysis reports, graphics analysis reports, MICF inquiries, and exception reports that you can either use as delivered or tailor to meet your specific requirements. Each type of report and reporting facility is described in the following pages.

Standard Analysis Reports

You can use standard analysis reports in conjunction with the usage guidelines to provide a structured approach to analysis. The standard analysis reports, delivered with this product and described in the following chart, can be grouped into four types:

- o Service analysis reports
- o Workload analysis reports
- o Data collection reports
- o Network incident reports

You can produce reports in both profile and trend versions. The profile version displays information for a single time period while the trend version displays trend information for several data periods (for example, percentage change) to help you spot patterns.

Service Analysis Reports	Function

Service by Application	Indicates the level of network and host service that the network provides to a given primary logical unit (PLU). This report can help you determine whether a response time problem is network-wide or is limited to a single application, and whether the degradation results from delays within the host or within the transmission media.
Service by Link	Quantifies the service that the network provides to users of a given boundary

link. This report can help you determine whether a network performance problem is limited to a given link.

Service by Performance Class Quantifies the service that the network provides to a given user group identified by performance class. If the performance classes conform to the classification specified in your service level agreements, this report can help you track your adherence to your service commitments.

Service by Control Quantifies the service that the network provides to a control unit, which helps you track performance with respect to control units.

Service by Terminal Quantifies the service that the network provides to a given terminal (SLU) when in session with a particular application (PLU), which can help you track end user response time for individual terminals and to identify occurrences of excessive host, network, or total response time.

Workload Analysis Reports	Function

Workload by Application	Quantifies the workload volume imposed on the network by a given host application, which can help plan for future growth or change in the application.
Workload by Link	Quantifies the workload volume imposed on the network by the devices attached to a given boundary link, which can help you plan for changes in your network configuration.
NPM/NetSpy Utilization by NCP	Identifies and quantifies potential capacity-related bottlenecks in the network's "backbone" NCPs, which can help identify the approach of the maximum supportable utilization level.
NPM/NetSpy Utilization by Link	Identifies and quantifies potential network link over-utilization conditions.
Workload by Control Unit	Quantifies workload volume for each monitored terminal controller (physical unit), which can help you recognize the approach of the maximum supportable utilization level.
Workload by Terminal	Quantifies the workload volume imposed on the network by the devices attached to a given terminal, which can help you identify the heaviest users of network resources and plan for changes to your network configuration.

Data Collection Reports	Function
NPM/NetSpy NCP Link Data Collection	Identifies network resources for which NPM network data or CA NetSpy NCP interface data was collected. This report identifies the scope of either NPM network data collection or CA NetSpy NCP interface data collection.
NPM Session Data Collection	Identifies network resources for which NPM session data was collected. This report identifies the scope of NPM session data collection.
NPDA Event Analysis	Identifies network resources for which NetView Hardware Monitor or CA NetMaster Network Error Warning System logged a permanent failure, which can help you plan for required network support personnel and schedule preventive maintenance.
NPDA Statistics Analysis	Identifies network resources for which NetView Hardware Monitor or CA NetMaster Network Error Warning System logged temporary errors, which can help you analyze the cause of intermittent network performance degradation, and schedule preventive maintenance for those devices with a potential for failure.

Graphics Analysis Reports

CA MICS Network Analyzer Option can produce graphics that include color plots, charts, and other screen and plotter displays. The sample graphics that are provided are particularly useful for displaying trends and comparisons and for quickly identifying potential problem areas.

The samples consist of 11 SAS routines that produce color graphics inquiries. You can use these inquiries for service, workload, and reliability analysis. The basic routines are structured so that you can easily modify them to meet your data center's needs. Sample graphics distributed with CA MICS Network Analyzer Option are described next.

Reports	Function
Average Response Time by Performance Class	Determines adequacy of service to end users based on user-defined performance classifications. A reference line on the graph indicates the objective response time for the performance class.
Application Service Analysis by Hour	Determines amount of host vs. network response time an application consumed.
Application Service Analysis	Determines amount of response time consumed on the host compared to that consumed by the network for comparable applications.
Response Objective Results by Performance Class	Establishes response objectives to provide measures of service, which shows how close you came to meeting objectives for a given performance class.
Traffic Profile Report for Link	Determines traffic load variation on a link over the course of a day and indicates the portion of the load that is due to data retransmission.
Communications Controller Utilization	Determines the communications processor load variation over the course of a day.
NCP Buffer Utilization	Helps determine adequacy and utilization of memory in the communications control unit (CCU).

Percent Link Utilization	Determines traffic fluctuation on a link over time, which can help you analyze the need for changes to the configuration, such as addition of links or upgrading of link speed.
Error Count for Link	Shows changes in line quality over the course of some period of time.
Percent Temporary Errors to Traffic	Shows the percentage of temporary errors to total line traffic as reported by the NetView Hardware Monitor.
NPDA Events for Cluster Controller	Shows the number of site-defined events that NetView Hardware Monitor or the CA NetMaster Network Error Warning System recorded each hour of a time period.

MICF Inquiries

The CA MICS Information Center Facility (MICF) allows you to access and manipulate data in the CA MICS database. MICF minimizes your need to write SAS code and, since you write less code, minimizes SAS syntax errors. MICF also provides automatic validation procedures that prevent you from attempting to analyze data elements that do not exist in the files you request.

CA MICS Network Analyzer Option contributes over 50 inquiries to the MICF library. The inquiries provide useful reporting and color graphics output that you can tailor through execution time parameters. You can also modify copies of the distributed inquiries to customize reports to your specific needs.

Inquiries distributed with this product can be grouped into four types:

- o Service analysis inquiries
- o Reliability analysis inquiries
- o Performance analysis inquiries
- o Workload analysis inquiries

The MICF inquiries that are delivered with the CA MICS Network Analyzer Option are described in the following charts.

Service Analysis Inquiries	Function
Application Service/ Workload Ranking	Ranks all or selected applications in ascending or descending order by selected service or workload criteria, and displays service and workload measures associated with the application.
Daily Average Response by Performance Class	Indicates adequacy of service to end users based on site-defined performance classes. A reference line shows objective response time for the performance class.
Daily Percent Response Objectives by Performance Class	Illustrates how close you came to meeting objectives for a user-defined performance class.
NetView Daily Aver- age Response by Link	Shows average end user response time for all terminals attached on a link to a terminal control unit equipped with an IBM Response Time Monitor, and summarizes average response time independent of performance classes defined in NetView Session Monitor for terminal-to-host sessions across the link. This chart can help you determine which links offer the shortest or longest average response times.
NetView Daily Per- cent Response Within Objective by Link	Shows how close you came to meeting objectives for all performance classes defined for the terminal-to-host sessions across a given link. This chart summarizes the percent of response within objective across performance classes defined for terminal-to-host sessions on the link.
CA NetSpy Daily PLU Response Time Components	Determines, for an application, the portion of the average total response time that occurs in the host compared to the average total response time in

the network.

Service Analysis Inquiries	Function
TSO Response Time Components	Determines, for TSO, the portion of the average total response time that occurs in the host compared to the average total response time in the network.
CA NetSpy Daily SLU Response Time Components	Determines, for a terminal, the portion of average total response time that occurs in the host compared to average total response time in the network.
NetView Link Service/Workload Ranking	Ranks all or selected links in ascending or descending order by selected service or workload criteria, and displays service and workload measures associated with the link.
NetView Performance Class Service/ Workload Ranking	Ranks all or selected NetView performance classes in order by selected service or workload criteria, and displays service and workload measures associated with the application.
NPM Application/Link Service/Workload Ranking	Ranks all or selected application and link combinations in ascending or descending order by selected service and workload criteria, and displays service and workload measures associated with the application/link.

Reliability Analysis Function
Inquiries

NPM Daily Link Error Count	Shows the count of temporary errors the network control program detects in network line components during the measurement interval.
NetView Daily Percentage Link Errors to Traffic	Shows increases in the percentage of temporary errors to total line traffic over a 24-hour period.
NPDA Daily Resource Alert Summary	Identifies devices with the greatest number of alerts (either generic, standard, or statistical) for all NPDA monitored resources, including LAN-attached, channel-attached, remote-attached, and distributed hosts.
NPDA Daily Resource Alert Description	Shows alert descriptions and configuration information for resources with the greatest number of alerts. Includes generic and standard alerts for all NPDA monitored resources.
NetView Daily NPDA Events Summary	Shows events recorded because the percentage of temporary errors to line traffic threshold has been exceeded, or some other user-defined event has occurred.
NetView Events Ranking	Ranks all or selected NetView Hardware Monitor reported events in ascending or descending order by selected ranking criteria, based on the number of events or alerts recorded.
NetView Events by Resource Type Ranking	Ranks all or selected NetView Hardware Monitor reported events for each resource type in ascending or descending order by selected criteria, based on number of events or alerts recorded.
NetView Events by Resource Ranking	Ranks all or selected NetView Hardware Monitor reported events for each network resource in user-determined order by selected ranking criteria, based on

number of events or alerts recorded.

Reliability Analysis Function
Inquiries

NetView Weekly Abnormal UNBINDs	Records, by PLU, the number of abnormal UNBINDs that occur for sessions with each PLU during the week.

NetView Weekly Abnormal UNBIND Report	Identifies, by PLU, the 20 SLUs that had the highest number of abnormal UNBINDs for the week.

Performance Analysis Function
Inquiries

Daily Percentage of NCP Cycle Utilization	Determines the communications processor load variation (communications controller utilization cycles) for a 24-hour period.

Daily NCP Buffer Utilization	Helps you determine the adequacy and utilization of NCP storage in the communications control unit.

Daily Link Utilization	Determines the traffic fluctuation on a link for a 24-hour period, which can help you determine the need for configuration changes such as adding links or increasing link speed.

NPM/CA NetSpy Under/Over Utilized Line Analysis	Identifies, through a series of four reports, which lines in the network are under-, over-, or marginally utilized.

NCP Utilization Ranking	Ranks all or selected NCPs in ascending or descending order by selected criteria, based on average, maximum, or minimum NCP buffer or CCU utilization, or the amount of time in slowdown.

NPM/CA NetSpy Daily Link Ranking By Zone	Ranks all or selected links in ascending or descending order based on sending, receiving, or total percent link busy.

NPM/CA NetSpy Daily Link Ranking	Ranks all or selected links in ascending or descending order based on

By Hour

sending, receiving, or total percent
link busy.

Performance Analysis Inquiries - continued

Performance Analysis Function
Inquiries

NCP Utilization Chart	Provides a bar chart of average hourly percent CCU and NCP buffer utilization and time in slowdown for each hour of day reported.
NCP Utilization Plot	Plots average hourly percent CCU and NCP buffer utilization and time in slowdown for each hour of day reported.
NCP Channel Hold and Intermediate Queue Length Plot	Plots NCP channel hold and channel intermediate queue lengths for each hour of a day reported, which can help you identify periods of excessive delay in data flow between NCP and VTAM.

Workload Analysis Function
Inquiries

NetView Daily Connect Time by Application	Shows total network terminal connect hours for each application.
NetView Daily Characters/1000 by Application	Shows volume of data character traffic for each application, which can help you determine traffic workloads placed on the network by total traffic to and from a given application.
NetView Daily Data Characters/1000 by Virtual Route	Shows traffic load variation on a virtual route for a 24-hour period, which can help you plan routes and balance loads during peak hours.
NetView Daily Data Characters/1000 by Application	Shows volume of data character traffic for each application, which can help you identify peak activity periods that may correlate with poor response time or low activity periods, possibly indicating network or host problems.
TCP/IP Daily Byte Transfer Chart	Provides a chart of bytes received and bytes sent by the TCP/IP Telnet Server for each hour of a day for a specific host/system.

TCP/IP Monthly Byte Transfer Chart	Provides a chart of bytes received and bytes sent by the TCP/IP Telnet Server for each zone by month for a specific host/system.

MICF Inquiries - continued

Workload Analysis Inquiries	Function
NetView Daily Control Characters/1000 by Application	Displays control character traffic volume for each application that you can compare with the MICF inquiry NetView Daily Data Characters/1000 by Application to determine the ratio between data and control characters.
NetView Weekly Control PIU Traffic by PLU	Shows control message volumes for individual PLUs that you can compare with the NetView Weekly Data PIU Traffic by PLU inquiry to determine the ratio between data and control PIUs.
NetView Weekly Data PIU Traffic by PLU	Shows data message volumes for individual PLUs that can help you determine traffic workloads imposed by individual applications on the network.
NetView Daily Link Rank Report	Identifies links with long average message lengths that would benefit most from a reduction in message sizes or from a compression in software.
NetView Daily PLU Rank Report	Identifies applications that would benefit most from a reduction in message sizes or from a compression in software.

Exception Reports

The CA MICS platform provides an Exception Analyzer that works with CA MICS Data Integration Applications (DIAs) to provide consolidated reporting of exception conditions across systems and data sources.

An "exception" is any condition that deviates from the expected norm, or any missed objective in system performance or service. DIAs detect exceptions by testing daily data against user-defined thresholds. Each application has an exception value analyzer to help determine those thresholds.

Each detected exception is assigned a severity level and is

associated with a management area. CA MICS Network Analyzer Option is delivered with several exception tests, and you can easily add your own. The exception reports produce increasing levels of detail to address the needs of different audiences and, when combined with exceptions from other CA MICS applications, comprise a powerful diagnostic tool for your organization.

Ad Hoc Reporting Facilities

The specific types of information needed to manage a large I/S organization change daily. CA MICS addresses those needs with interactive capabilities that allow fast response to the most complex requests for information. The interactive capabilities are:

- o The CA MICS Information Center Facility (MICF) is an ISPF-based panel-oriented productivity tool that allows you to access information in the CA MICS database. When you define input, selection criteria, and report options, MICF fulfills your request executing the program either in batch or interactive mode. Then, according to your specifications, MICF either prints the results of your request, displays the results at your terminal, or catalogs the results for later viewing.
- o The standard SAS Language Interface is an advanced analysis language that enhances your staff's analytical capabilities and improves the quality of their decision-making. CA MICS uses SAS, a powerful fourth generation language that allows easy data manipulation and statistical analysis. SAS also provides coding facilities for programmers who are conducting extensive analysis or designing new reports for I/S business applications.

The CA MICS WorkStation Facility (MWF) provides an online environment in which you can use SAS in batch or interactive mode. CA MICS uses the SAS System for data management and as an advanced analysis language.

1.4 Files Overview

CA MICS Network Analyzer Option supports data from the following commercially available network monitor products:

- o CA NetSpy Network Performance
- o CA NetMaster Network Management for SNA
 - Network Tracking System (NTS)
 - Network Error Warning System (NEWS)
- o IBM TCP/IP for z/OS
- o Tivoli NetView Performance Monitor (NPM)
- o Tivoli NetView Session Monitor (NLDM)
- o Tivoli NetView Hardware Monitor (NPDA)

Information from these products is grouped into three information areas:

- o The NVS Information Area contains information about NetView sessions in the following files:

- NVSLSY - NLDM System (PLU) Activity File
- NVSNLL - NLDM Link Activity File
- NVNSA - NLDM Session Accounting File
- NVNSC - NLDM Session Connectivity File
- NVSRTE - NLDM Route File
- NVSRM - NLDM Response Time File
- NVSVBF - NLDM VTAM Bind Failure File

For file descriptions, see chapter 5.

- o The SNT Information Area contains information about networks in the following files:

- SNTCAF - Network Components Activity File
- SNTGAF - NPDA Generic Alert File
- SNTLNF - NPDA LAN File
- SNTNAC - NCP Network Accounting File
- SNTNAF - NCP Activity File
- SNTNCL - NCP Link File
- SNTNEF - NPDA Event File
- SNTNIN - Network Incident File
- SNTNLP - NCP Line Processor Activity File
- SNTNPL - NPM Link Activity File
- SNTNSF - NPDA Statistical File

SNTNSP - CA NetSpy Application PLU File
 SNTNSS - CA NetSpy Terminal SLU File
 SNTNSV - NLDM Service File
 SNTNTS - Telnet Server Entry File
 SNTNVR - CA NetSpy Virtual Route Activity File
 SNTPSU - NPM User Activity File
 SNTPSY - NPM System (PLU) Activity File
 SNTTCS - Stack Entry File

For file descriptions, see chapter 5.

- o The TCP Information Area contains information about IBM's TCP/IP services in the following files:

TCPSTN - Telnet Server File
 TCPCTN - Telnet Client File
 TCPFSF - FTP Server File
 TCPFCF - FTP Client File
 TCPFLF - FTP Login Failure File
 TCPAPI - API Calls for Sockets File
 TCPPIX - IP Statistics File
 TCPICX - ICMP Statistics File
 TCPTCI - TCP Statistics File
 TCPUDI - UDP Statistics File

For file descriptions, see chapter 5.

Figure 1-2 illustrates the relationship between data sources and files.

Data	
Source	CA MICS Network Analyzer Files
CA NetSpy	SNTCAF, SNTNAC, SNTNAF, SNTNCL, SNTNIN, SNTNSP, SNTNSS, SNTNVR, SNTNTS, SNTTCS
NPM	SNTCAF, SNTNAC, SNTNAF, SNTNCL, SNTNIN, SNTNPL, SNTPSU, SNTPSY
NLDM	NVSLSY, NVSNLL, NVNSC, NVNSA, NVSRTE, NVSRMT, NVSVBF, SNTNSV
NPDA	SNTGAF, SNTLNF, SNTNEF, SNTNSF
NTS	NVSLSY, NVSNLL, NVNSA, NVNSC, NVSRTE, NVSRMT, NVSVBF, SNTNSV

NEWS	SNTNEF, SNTNSF
TCP	TCPSTN, TCPCTN, TCPFSF, TCPFCF, TCPFLF, TCPAPI, TCPIPX, TCPICX, TCPTCI, TCPUDI

Figure 1-2. Data Sources and Files

1.5 Product Prerequisites

CA MICS Network Analyzer runs in a CA MICS environment operating under z/OS.

In addition, you will need at least one of the CA MICS supported network monitors listed in Section 1.4.

1.6 Benefits

CA MICS Network Analyzer contributes to the overall benefits that CA MICS provides. Those benefits fall into the following broad categories:

- o Improves day-to-day management
- o Reduces risk to the enterprise
- o Controls and/or helps reduce costs
- o Improves return on the I/S investment
- o Increases productivity
- o Improves planning

The material below explains how the CA MICS Network Analyzer contributes to these benefits.

Improves Day-to-day I/S Management

- o Tracks problem symptoms and supplies information so that you can take corrective action
- o Highlights recurring, persistent performance and response issues that require further analysis, tuning, or planning
- o Helps to identify reliability issues and trends to allow you to focus on vendors or products that are providing poor performance

Reduces Risk to the Enterprise

- o Provides more accurate and complete information than is available from any single network monitor application
- o Ensures complete and non-redundant configuration data for cross-domain sessions when NetView is active and producing data in both domains
- o Improves insight into problems that can affect important users
- o Provides the flexibility and open-ended architecture to adapt to technological change

Controls and/or Helps Reduce Costs

- o Permits you to charge back all resources
- o Provides flexibility in chargeback
- o Educates users about resource costs and usage patterns

Improves Return on the I/S Investment

- o Provides you with the ability to equitably charge users for resources
- o Provides better information with which to justify decisions, and to more effectively present positions and proposals

Increases Productivity

- o Incorporates data from multiple networks into the same database, while retaining the ability to analyze each network separately
- o Standardizes reporting, thus reducing problem analysis time
- o Provides the potential to combine data from two or more domains in different time zones, thus simplifying analysis
- o Allows you to use resources more effectively and efficiently

Improves Planning

- o Helps you to identify and perform basic analysis on utilization trends that point towards eventual saturation of network components
- o Supplies you with the means for evaluating hardware and software prior to making a commitment for acquisition

Chapter 2: USAGE CONSIDERATIONS

This chapter describes guidelines for the presentation, interpretation, and application of the data made available by the CA MICS Network Analyzer. An overview of the scope and general areas of application of the Analyzer's data is presented, followed by a more detailed discussion of terminology, concepts, components, and data flow as they relate to the available data.

An introduction to the generalized CA MICS Information Structure will acquaint you with the relationships among CA MICS data sources. Subsequent sections target the specific data archived by CA MICS within this overall structure.

Finally, specialized analyses, sample SAS code, and data manipulation guidelines are provided.

This section contains the following topics:

[2.1 Introduction to the Use of Network Data](#) (see page 40)

[2.2 General Analysis Considerations](#) (see page 42)

[2.3 Use Within the Information Structure](#) (see page 82)

[2.4 Specialized Analysis](#) (see page 146)

[2.5 Data Manipulation Guidelines](#) (see page 153)

[2.6 Multiple Session Manager Considerations](#) (see page 156)

2.1 Introduction to the Use of Network Data

Today, almost no large installation can function without sophisticated data communications capabilities. Those requirements pervade the organization so completely that inadequate performance of the communications facilities can adversely affect the profitable operation of the business. Because of this dependence, it has become mandatory for organizations to make a conscious effort to manage their communications networks systematically.

The management of large-scale communications networks is a difficult task because communications is an integral part of so many divergent activities. The scope of resources, vendors, applications, hardware types, tools, problems, and users exceeds that of any other group in the data center.

This management effort is further hampered by the lack of an established methodology (such as exists within the mainframe environment) for performance evaluation, tuning, and capacity planning. Until recently, there existed a shortage of comprehensive network measurement tools capable of producing usable network management information.

IBM and other vendors have addressed this lack of data with a series of network management products. However, these products lack integration, which can result in redundant network data.

CA MICS addresses this problem by:

- o Providing a common database to support the multitude of data sources
- o Integrating network monitor data with application monitor data
- o Supporting a network management methodology that is integrated with an overall installation management methodology

- o Supplementing the existing monitor data with calculated and user-specified characterization data to increase its usability
- o Producing a variety of tabular management reports which are not available from the network monitor products
- o Providing analysis of network data using CA MICS exception monitoring and reporting.

The network monitor products produce three broad categories of data:

- o Network Load and Utilization Data
- o Network Response Time Data
- o Network Reliability Data

Network load and utilization data consists of command, path information unit (PIU), and character counts by logical unit (LU), physical unit (PU), link, application, and so on. This data can be summarized to indicate the amount of network load that is supported or generated by a given network element. Link workload may be expressed as a function of link bandwidth (speed), thus yielding a percentage utilization figure. Percentage of link utilization reported over time for key network links can be used to anticipate the development of bottlenecks and estimate the magnitude of required upgrades.

Network response time data consists of host, network, and total response times by LU, PU, link, application, and performance class. These network service statistics can be analyzed in light of installation standards and industry accepted values to indicate the adequacy of end-user service. Service degradation can be identified as residing in the network or in the host processor. In many cases, service problems can be isolated to a given network application, path, or component, thus limiting the scope of activity in formulating a solution.

Network reliability data consists of error statistics, events, and alerts resulting from hardware component malfunctions. Error statistics are made up of temporary error counts and network traffic information. Events are recorded when the ratio of temporary errors to traffic exceeds an installation-defined threshold or when a permanent

error occurs. Alerts are recorded for installation-defined error conditions of extreme concern. Additional reliability data is provided in the form of errors which result in premature UNBIND conditions between primary and secondary logical units.

2.2 General Analysis Considerations

This section is a functional overview of IBM's Systems Network Architecture (SNA) and an overview of TCP/IP (Transport Communication Protocol/Internet Protocol). It provides you with a framework for the application of the CA MICS data. This overview is presented from a data analysis viewpoint and is not intended to be a comprehensive primer on the SNA architecture or product line.

The following sections discuss specific aspects of SNA:

- 1 - Pre-SNA Communications
- 2 - SNA Overview
- 3 - Comparison of SNA and the OSI Model
- 4 - TCP/IP Overview

2.2.1 Pre-SNA Communications

SNA-based communications networks are made up of elements that combine hardware and software to perform a single logical function. Before SNA development, IBM networks were made up solely of hardware elements. Because much of the terminology of the pre-SNA environment (e.g., terminal, line control unit, etc.) is still commonly (and often preferentially) used to refer to SNA network elements (e.g., logical units, links, physical units, etc.), confusion exists as to the actual meaning of the SNA terms. This section briefly reviews the evolution of data communications in the IBM environment in an attempt to relate SNA concepts to common experience.

Unlike some other mainframe architectures, the System 360 architecture did not inherently provide for terminal communication within its basic design. Thus, when terminal communications were desired, IBM engineers were faced with the problem of interfacing the IBM channel, a high bandwidth (data carrying capacity), low addressability, data transfer mechanism, to a potentially large number of independent terminals which randomly generated small bursts of traffic.

To accomplish this, IBM engineers developed a device, the 2701 Transmission Control Unit (TCU), consisting of three hardware elements:

- o Channel Interface -- communicates with the IBM channel
- o Transmission Interface Converter -- handles internal communication between the Channel Interface and the Transmission Adapter.
- o Transmission Adapter -- handles terminal-dependent and line activities

```

      +-----+ C
--- I ---| C  I  | T  I  C  | T  A  | O
--- B ---| H  N  | R  N  O  | R  D  | M
--- M ---| A  T  | N  T  N  | N  A  | ---
---    ---| N  R  | S  R  V  | S  P  | /
--- C ---| N  F  | M  F  E  | M  T  | ---
--- H ---| E  A  | I  A  R  | I  E  | L
--- A ---| L  C  | S  C  T  | S  R  | I
--- N ---|      E  | N  E  R  | N      | N
      +-----+ E

```

Figure 2-1. 2701 Transmission Control Unit

The 2701 TCU was the forerunner of today's 37xx Communication Control Units. It performed five basic functions which are still central to data communications in an SNA environment:

- o Decoded IBM channel commands
- o Performed conversion from the channel (parallel data stream) to the communications line (serial data stream)
- o Recognized line control characters
- o Provided transmission error checking
- o Provided status and sense information to the IBM channel

The development of multiple terminal types, each with special transmission control requirements, necessitated the design of a number of specialized transmission adapters. The desire to reduce the required inventory of hardware and increase the number of terminal types which could be supported resulted in the design of the programmable 3705 Communications Control Unit.

The 3705 performed essentially the same functions as its predecessor, but the transmission adapter function was implemented in software modules called Emulators because they performed the function of the 270x transmission adapter hardware. The transmission interface converter function was also implemented in software. The software executed on a specialized processor called the central control unit, which accessed both a parallel data path (IBM channel) and a serial data path (communications line) via peripheral devices. The addition of software components to the transmission control unit function and the resultant flexibility prompted the proliferation of the hardware-software element philosophy evident in SNA.

```

      +-----+ C
--- I ---| C  A  | C  C  U  | C C S  | O
--- B ---| H  D  | E  O  N  | O A C  +--| M
--- M ---| A  A  | N  N  I  | M T A  |L |---
---    ---| N  P  | T  T  T  | M I N  |I | /
--- C ---| N  T  | R  R    | U O N  |B | ---
--- H ---| E  E  | A  O    | N N E  +--| L
--- A ---| L  R  | L  L    | I S R    | I
--- N ---|      | (PROCESSOR) | -      | N
      +-----+ E

```

Figure 2-2. 3705 Communications Control Unit

The programmable communications control unit reduced the effort and cost of supporting new terminal types, but major changes in terminal hardware still affected the entire network. The designers of SNA worked to reduce the scope of a given change by isolating the logical functions of communications into layers joined by well-defined interfaces. These interfaces could only be maintained through the use of combined hardware-software elements.

Thus, at its basic level, SNA can be viewed as simply the application of structured design techniques to the task of data communication. The confusion between SNA and pre-SNA terminology results from the lack of distinction between a given piece of hardware and the logical SNA functions it implements. The following sections of this chapter discuss these logical functions in detail.

2.2.2 SNA Overview

IBM's Systems Network Architecture (SNA) is a collection of standards which define in detail the requirements for communications within an IBM network. SNA is not a product in itself, although many of the standards which comprise SNA are implemented in hardware and software products marketed by IBM and other vendors. Not all of the features and facilities defined by SNA are currently implemented in products; also, additions to the architecture are made frequently (usually with the implementation of a new product). Thus any description of SNA is limited by the necessity to describe a "snapshot" of an evolving entity in terms of the products that are currently implemented. Such a description is presented, without further apology, herein.

In the most general terms, SNA is a hierarchy consisting of seven layers. Each layer performs a specific function consisting of one or more services for the next higher layer. In turn, each layer requests services from the next lowest layer and communicates with peer layers throughout the network. Because the layers are functionally self-contained, most changes to a layer are restricted to that layer. Only changes to the interface between layers can affect another layer and then only the next higher layer is affected. Figure 2-3 shows a diagram of the seven SNA layers.

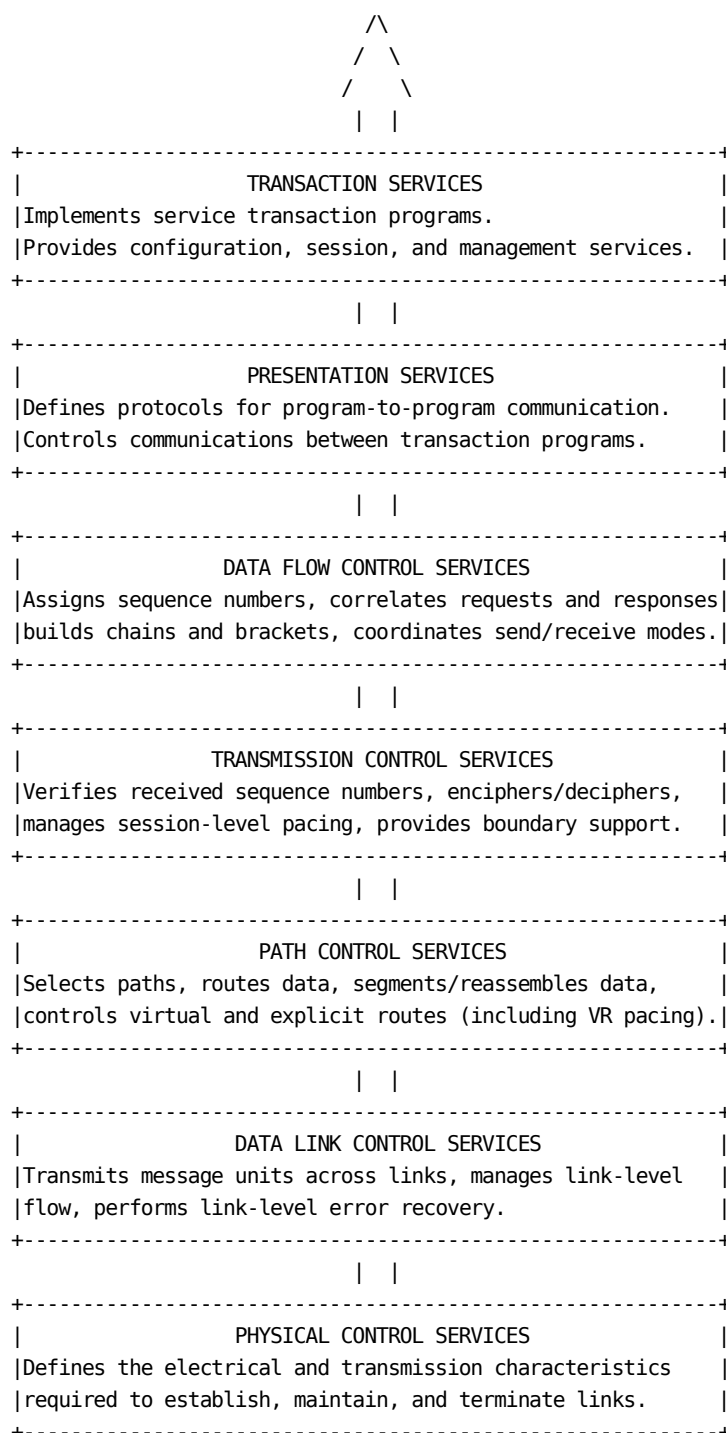


Figure 2-3. The Seven SNA Layers

The functions of the seven architectural layers of SNA are implemented by combinations of hardware and software components. Hardware components include the following:

- o Host Processors (mainframes)
- o Communications Controllers (37XX and equivalents)
- o Cluster Controllers (3274, etc.)
- o Workstations (3278, etc.)
- o Printers (3287, etc.)

Software components include the following:

- o Telecommunication Access Methods (ACF/VTAM, etc.)
- o Application Subsystems (TSO, IMS, CICS, etc.)
- o Network Control Programs (ACF/NCP, etc.)

These components are defined and discussed in greater detail in the following sections:

- 1 - SNA Terminology
- 2 - SNA Network Design Fundamentals
- 3 - SNA Session Activation and Termination

2.2.2.1 SNA Terminology

Some special terms are used to refer to the hardware and components that implement the SNA architecture. Therefore, a basic understanding of these terms is germane to any discussion of SNA. This section presents several key terms and their definitions.

In general, entities in an SNA network represent functions rather than things. Therefore, most of the terms defined below identify combinations of hardware and software. In some cases, the software or hardware component of a specific network element has not been explicitly mentioned to make the definition more readable.

Figure 2-4 illustrates a sample relationship among nodes, links, and subareas.

NODES

An SNA network is made up of NODES which are connected to one another by one or more LINKS. An SNA node is that portion of a hardware component and its associated software components that implement the functions of the seven SNA layers. The architecture currently defines three types of nodes: host subarea nodes, communications controller subarea nodes, and peripheral nodes.

HOST SUBAREA NODES

A host subarea node consists of a processor containing a telecommunications access method such as VTAM. These nodes provide the control and management functions for the network.

COMMUNICATIONS CONTROLLER SUBAREA NODES

A communications controller running a network control program such as ACF/NCP makes up a communications controller subarea node. These nodes provide data routing and flow control for the network.

PERIPHERAL NODES

Numerous devices including cluster controllers (3274s, etc.), distributed processors (8100s, etc.), workstations (3178s, PCs, etc.), and printers (3287s, etc.) are peripheral nodes. They provide network access and

services for the end-user.

SUBAREAS

A subarea consists of one host or communication controller node and the peripheral nodes that are attached to it. Subareas are the major breakdown of the network for routing. Messages originating in a peripheral node in one subarea and bound for a peripheral node in another subarea are routed first to the destination subarea and from there to the appropriate peripheral node.

CA MICS Network Analyzer identifies the subarea number associated with the session partners in files created from NPM data as follows:

- o Primary Logical Unit Subarea - PLUSA
- o Secondary Logical Unit Subarea - SLUSA

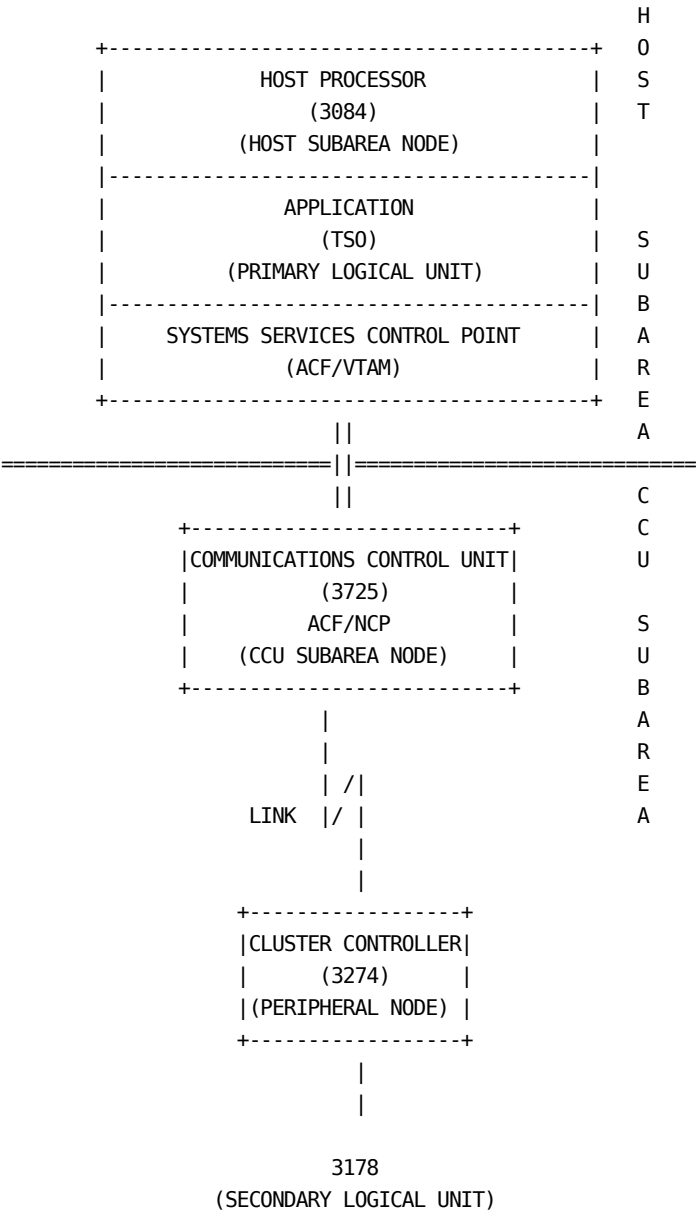


Figure 2-4. Network Nodes, Links, and Subareas

LINKS

Links are the media through which adjacent nodes are connected. A link consists of a link connection and two or more link stations.

LINK CONNECTIONS

The physical medium of transmission between two nodes is called the link connection. These may be telephone wires, fiber optic cables, microwave beams, System 370 channel cables, etc.

LINK STATIONS

The combination of hardware and software that allows a node to attach to, and provide control for, a link is a link station. Link stations transmit data over a link using data link control protocols.

TRANSMISSION GROUPS

Transmission groups (TGs) are groups of one or more links connecting adjacent nodes that are defined logically to the path control network as a single link. Use of transmission groups allows an installation to match the bandwidth (capacity) of a path to the requirements (i.e., as traffic increases, additional lines can be added to the transmission group). Transmission groups also tend to exhibit higher availability than individual links because if one link of a multi-link TG fails, the connection is not lost.

PERIPHERAL LINKS

Peripheral links connect a subarea node and a peripheral node. Since peripheral nodes are placed at the logic extremities of the network, these links are sometimes called boundary links. CA MICS Network Analyzer retains the peripheral link name in the data element SLULINK in many files.

NETWORK ADDRESSABLE UNITS (NAUs)

Network addressable units are sources, destinations, or elements in the path of network traffic. Network addressable units provide end-user access to the network and aid network operators in management and control functions. Each NAU has an associated address that the path control network uses to route data to it. There are three types of NAUs:

- o Logical Units (LUs)
- o Physical Units (PUs)
- o System Services Control Points (SSCPs)

LOGICAL UNITS (LUs)

Logical units are the access points to the network. End-user communication over the network is possible only when the respective end-user's LUs establish a mutual relationship called a session. Not all LUs support the same set of SNA functions; the architecture uses LU type to identify the supported functions. Currently seven LU types exist:

- o LU Types 2, 3, 4 and 7 support communications between application programs and various types of workstations.
- o LU Types 1, 4, 6.1, and 6.2 support communications between two programs.

CA MICS Network Analyzer classifies logical units into one of two types:

- o Primary Logical Units (PLUs)
- o Secondary Logical Units (SLUs)

The primary logical unit is responsible for activating the LU-LU session. The secondary logical unit receives the BIND Session Request. Generally, PLU names identify host applications (TSO, CICS, IMS, etc.) and SLU names identify terminals.

PHYSICAL UNITS (PUs)

Physical units are the hardware elements of the network. Every SNA node contains one physical unit to manage the links connecting the node to other nodes. CA MICS Network Analyzer identifies several types of physical units:

- o Secondary Logical Unit Physical Unit (SLUPU)
- o Primary Logical Unit Subarea Physical Unit (PLUSAPU)
- o Secondary Logical Unit Subarea Physical Unit (SLUSAPU)

Secondary logical unit physical unit (SLUPU) names typically identify terminal control units. Primary logical unit subarea physical unit (PLUSAPU) names usually specify the host processor in which the application resides. The secondary logical unit subarea physical unit (SLUSAPU) names the host processor or communications controller node in which the SLU resides.

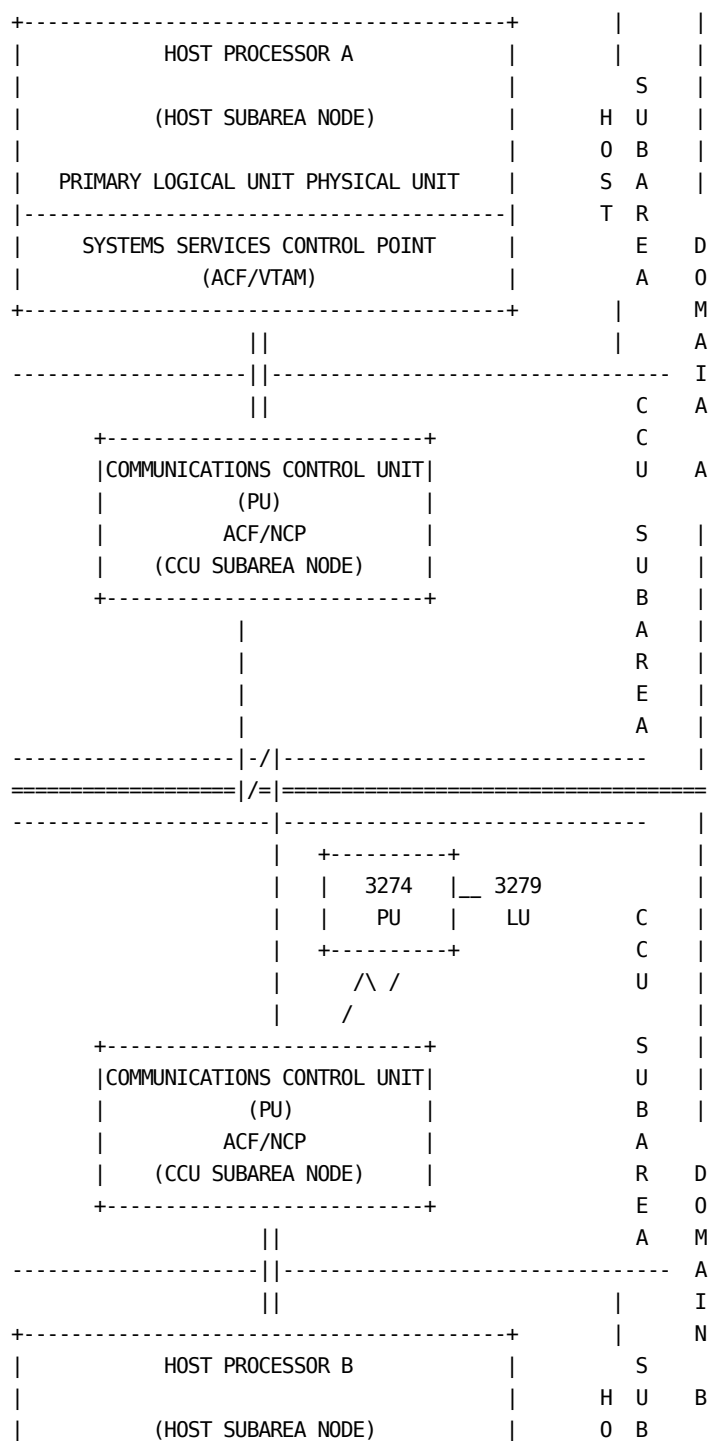
SYSTEMS SERVICES CONTROL POINTS (SSCPs)

Systems services control points are the functions within host subarea nodes which activate, control, and deactivate network resources. The physical location of the SSCP is a host processor, but the SSCP itself is a logical entity.

DOMAINS

The span of control of an SSCP is called its domain. A domain consists of one SSCP and the network resources (LUs, PUs, links, and link stations) that it controls. In some cases, network resources are shared by multiple SSCPs and thus reside in multiple domains. Resource sharing increases overall network availability by reducing the dependence on a single SSCP.

Figure 2-5 illustrates the relationships among domains, subareas, and logical and physical units.



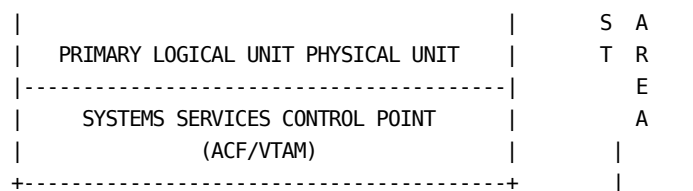


Figure 2-5. Network Addressable Units

The following sections discuss the addressing scheme used by SNA to refer to the various components discussed above, the protocols used to control the exchange of data at the seven SNA functional levels, and the message formats used to pass data between them.

- 1 - SNA Network Addressing
- 2 - SNA Data Formats
- 3 - SNA Protocols

2.2.2.1.1 SNA Network Addressing

Names and addresses are assigned during system generation to identify network resources to end-users and the path control network. Two levels of addressing are used by the path control network:

- o Network Addresses - used to route messages between subareas and between NAUs in subarea nodes
- o Local Addresses - used to route messages between subareas and peripheral nodes, and between NAUs in peripheral nodes

NETWORK ADDRESSES

Network addresses uniquely identify NAUs (SSCPs, LUs, PUs, links, and so on). Network addresses are made up of two parts: the subarea address and the element address.

Subarea addresses contain the subarea number of the subarea Node. The subarea number is user-assigned at system definition.

Element addresses are unique only within a subarea. They are assigned during system generation, network reconfiguration, activation of switched resources, or initiation of parallel LU-LU sessions.

Extended addressing uses a 23-bit address field for the network address. The extended address is divided into 8 bits for the subarea address and 15 bits for the element address. Previous addressing schemes used a total of 16 bits for the network address with a user-selected length for the subarea portion.

LOCAL ADDRESSES

Local addresses uniquely identify NAUs within a peripheral node. These addresses are used only to identify resources within a peripheral node and are not the same as the element addresses discussed above.

Network addresses are translated to local addresses by the boundary function, which resides in the subarea node. Thus, the boundary function insulates the peripheral node from network address changes resulting from reconfigurations.

NETWORK NAMES

End-users avoid having to know network addresses by referring to NAUs by symbolic names. These names are translated into addresses for the path control network by directory services in the SSCP. The use of network names insulates the end-user from address changes in the network.

SNA NETWORK INTERCONNECTION (SNI)

SNA network interconnection allows end-users in two separate SNA networks to communicate with each other without requiring unique addresses of network names in both networks. The interconnection is effected by a gateway consisting of a gateway node and at least one gateway SSCP. Network addresses are translated by the gateway node and network names are translated by the gateway SSCP. To ensure that addresses and names are unique among interconnected networks, gateways prefix them with a network identifier. The network identifiers are uniquely assigned during system generation.

The CA MICS Network Analyzer Option distinguishes between interconnected networks by retaining the network name in a common data element, NETWRKID. For the CA MICS files derived from NPM data, NETWRKID may be set to the value of the NPM data field PLUNETID. An additional network identifier, SLUNETID, is carried in the CA MICS NPM User Activity File. The Network Identifier Exit Routine, SNTNIDRT, is explained in Section 7.3.4.

2.2.2.1.2 SNA Data Formats

Network elements use several different message-unit formats to exchange data among themselves. These formats are often referred to in discussions of communications and are outlined below.

BASIC INFORMATION UNIT (BIU)

Network addressable units (NAUs) communicate via basic information units (BIUs). BIUs are either requests or responses. Requests initiate an exchange; responses acknowledge the receipt of a request. Request BIUs are made up of a request header (RH) and a request unit (RU). Response BIUs are made up of a response header (RH) and a response unit (RU).

Request and response headers are three-byte fields which identify the type of data in the associated request or response unit. The request/response indicator bit distinguishes a response header from a request header.

Request units are variable length fields which contain either end-user data or an SNA command.

Response units are either positive or negative and contain information about the request. Positive acknowledgements to commands generally identify the command request. Positive acknowledgements to data requests contain no RU. Negative response units are four to seven bytes long and indicate why the request was not accepted.

PATH INFORMATION UNIT (PIU)

Path control elements exchange information via path information units (PIUs). PIUs are basic information units with a transmission header (TH) prefixing them. The transmission header contains the origin and destination NAU addresses, the explicit route number, and the virtual route number.

Transmission header formats vary depending on the type of nodes to which data is routed. The differences are indicated by the format identifier (FID) type.

- o FID 0 is used to route data between adjacent subarea nodes for non-SNA devices. This format is not now

commonly used.

- o FID 1 is used to route data between adjacent subarea nodes if one or both do not support explicit and virtual route protocols.
- o FID 2 is used to route data between a subarea node and an adjacent type 2.0 or 2.1 peripheral node or between directly connected type 2.1 nodes.
- o FID 3 was used to route data between a subarea node and a type 1 node.
- o FID 4 is used to route data between adjacent subarea nodes which support explicit and virtual route protocols.

BASIC LINK UNIT

Data link control uses basic link units (BLUs) to transmit data across links. A BLU consists of a PIU with a link header (LH) as a prefix and a link trailer (LT) as a suffix.

The various prefixes and suffixes are added and deleted as necessary as the message passes through the various SNA layers. Figure 2-6 shows the relationship between basic information units, path information units, and basic link units.

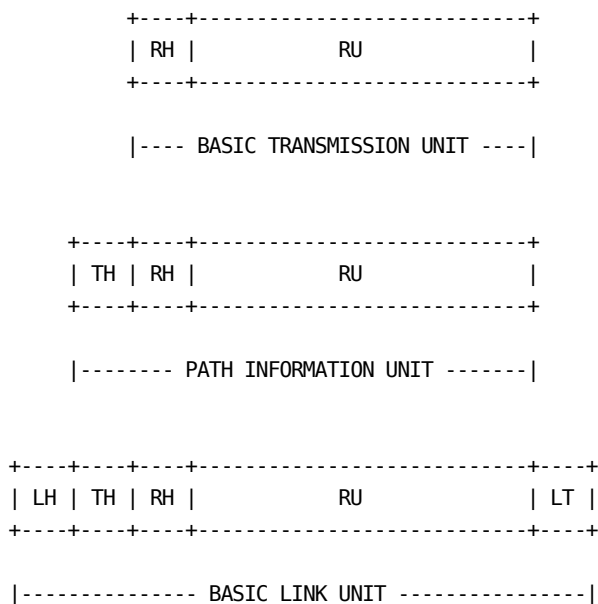


Figure 2-6. SNA Data Formats

It is these data formats that are exchanged within the SNA seven-layer hierarchy:

- o Presentation services (SNA Layer 6) in one node communicates with presentation services in another node by exchanging basic information units.
- o Path control services (SNA Layer 3) in the originating node communicates with path control services in the destination node by exchanging transmission headers which have been appended to the BIU to form a path information unit.
- o Data link control services (SNA Layer 2) in both nodes communicate via link headers and link trailers with which they frame the PIU to form a basic link unit.

2.2.2.1.3 SNA Protocols

Protocols are predetermined pairs of actions which are performed by two network elements to effect the exchange of data between them. For instance, when data transmission is initiated across an RS232 (EIA) interface, the sender raises DTR (data terminal ready) and RTS (request to send). When ready, the receiver responds with DSR (data set ready) and CTS (clear to send). RTS (request to send) is then toggled--high to send, low to receive--as messages are exchanged. The relationship between these four conditions and the exchange of data is a portion of the start/stop (asynchronous) data link control protocol.

The term protocol used alone, commonly refers to data link control protocols, but SNA networks also use path control network transmission protocols and BIND protocols. Common protocols within each of these groups are listed below.

DATA LINK CONTROL PROTOCOLS

Data link control protocols allow for the actual transmission of data bits across the physical medium. Common SNA DLC protocols include:

- o Synchronous Data Link Control Protocol (SDLC)
- o CCITT X.25 Protocol
- o Binary Synchronous Protocol (Bisync)
- o Start/Stop Protocol (Async)

PATH CONTROL NETWORK TRANSMISSION PROTOCOLS

Path control network transmission protocols allow the transmission rate to be maximized consistent with the capabilities of the NAUs being addressed. The three types of transmission protocols are:

- o Sequencing
- o Blocking
- o Segmenting

sequencing ensures that message units arrive at their destination in the same order they were sent. Order may be lost during transmission when the message units which make up a complete message are transmitted simultaneously on several links of a multi-link transmission group. Transmission group sequence numbers are used to reestablish the original order at the receiving end.

Blocking is used to combine PIUs into a single basic transmission unit (BTU). Blocking makes efficient use of a high-speed data channel. Figure 2-7 illustrates blocking.

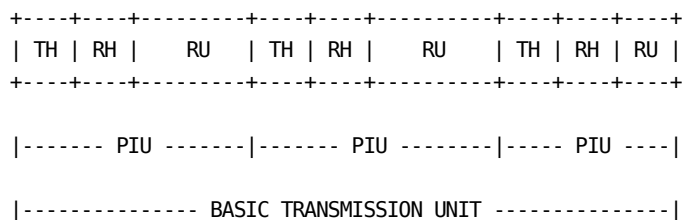


Figure 2-7. Blocked PIUs

Segmenting is used to divide a PIU into multiple shorter PIUs when the receiving node is not capable of processing the entire original PIU as a single unit. PIUs and BTUs are discussed in detail in Section 2.2.2.1.3, SNA Data Formats. Figure 2-8 illustrates the segmenting function.

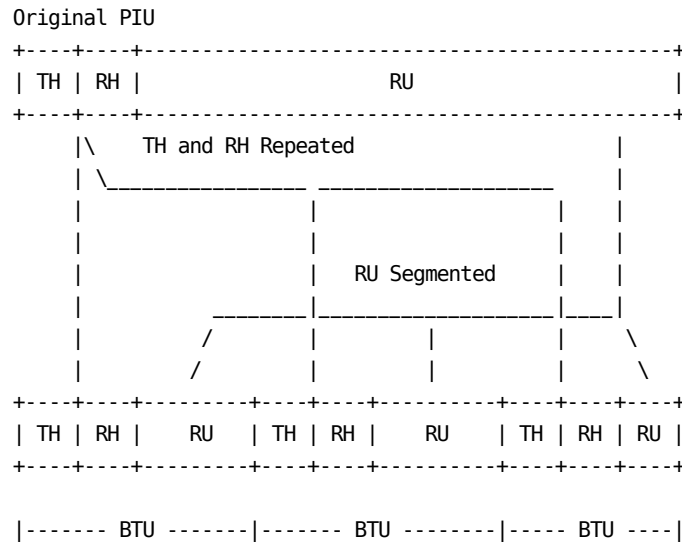


Figure 2-8. Segmented PIUs

BIND PROTOCOLS

BIND protocols define how logical units transmit data to one another and/or how that data is presented to the end-user. Various classes and types of BIND protocols are listed below:

o Response Protocols

Response protocols indicate how a receiver will acknowledge a sender's request. Three types of response protocols are defined:

- Definite Response

The sender sets either a DR1I or DR2I in the request header to identify the response protocol. The receiver must then return either a positive or negative response to accept or reject the request. Definite response causes extra link traffic. NPM uses the definite response to measure network

response time.

- Exception Response

The sender sets an ERI in the request header. The receiver then returns a negative response for any unacceptable requests; no positive responses are returned.

- No Response

The receiver does not return a response regardless of the acceptability of the request.

o Chaining Protocols

Chaining protocols allow a sender to initiate multiple transmissions in a single direction, which the receiver then treats as a single data transfer. This set of transmissions is called a chain. Chaining protocols may also require a response from the receiver, thus there are three types:

- Definite Response Chain

The sender sets ERI in the RH of all but the last request in the chain, where it sets DRxI. The receiver must then return either a positive or negative response to accept or reject the entire chain.

- Exception Response Chain

The sender set an ERI in the request header of all requests in the chain. The receiver then returns a negative response if there was an unacceptable request in the chain; no positive responses are returned.

- No Response Chain

The receiver does not return a response regardless of the acceptability of the chain.

o Bracket Protocols

Bracket protocols are used to separate groups of related chains from other groups of related chains. This facility is necessary to allow transaction programs to serially share a session between type 6.2 LUs.

o Sequencing Protocols

Sequencing protocols are used between session partners to ensure that related requests and responses are received in the same order that they are sent. Senders assign a sequence number of one to the first request sent following session activation. The sequence number is incremented by one for subsequent requests. The receiving LU assigns its responses the same sequence number as the corresponding request. Without

sequencing protocols, out-of-sequence conditions could develop if intervening network delays fluctuated.

o Request and Response Mode Protocols

Request and response mode protocols control the number of requests which can be outstanding for an LU-LU session. Four types of request and response mode protocols exist:

- Immediate Request Mode

The sending LU must wait for a response before sending additional requests. This applies only to requests specifying definite response. (Thus, an entire chain can be sent.)

- Delayed Request Mode

The sending LU does not have to wait for a response prior to sending additional requests.

- Immediate Response Mode

The receiving LU must return responses in the same order that it received the requests.

- Delayed Response Mode

The receiving LU can return responses in any order.

o Send and Receive Mode Protocols

Send and receive mode protocols determine when session partners can send requests. Three types are defined:

- Full Duplex

LUs can send and receive simultaneously.

- Half-Duplex Contention

Both LUs can send requests to each other, but not simultaneously. Contention (and lost data) occur if both LUs attempt to send at the same time. The BIND parameters identify a contention winner who is allowed to send its request first in this event (normally the terminal rather than the application is designated contention winner).

- Half-Duplex Flip-Flop

LUs alternate sending requests. BIND parameters designate one LU as first speaker. It sends the initial requests with a change direction indicator (CDI) in the last request header transmitted. The receiving LU becomes the sender upon receipt of the CDI. The LUs toggle between send and receive states by subsequent exchange of the CDI.

Note: these are not transmission medium protocols. LUs can operate in full duplex (i.e., sending and receiving) simultaneously even though some or all of the intervening transmission media can transmit data in only one direction at a time.

o Data Security Protocols

Data security protocols are implemented by logical units to prevent unauthorized access to end-user data. Three types of data security protocols currently exist:

- Passwords and User-IDs

A request carries a password and user-ID in an attach function management header. Verification of the password is implementation-defined.

- Session Cryptography

LUs can use the data encryption standard (DES) algorithm to encrypt and decrypt data. DES employs a randomly generated key methodology.

- LU-LU Session Passwords

Both the primary and secondary LUs can verify passwords prior to activating an LU-LU session. Each LU sends the other a random data string. The LUs then use their respective session passwords to encipher this data and return it to the other LU. The LU then enciphers the random data field it transmitted to the other LU using its own password. If the two enciphered fields match, both LUs are using the same password.

2.2.2.2 SNA Network Design Fundamentals

There are three objectives which must be satisfied in any network design:

- o Service
- o Availability
- o Efficiency

The relative importance of each of these factors determines (or at least should determine) the design of the network.

Service is usually measured by response time. Response time may be loosely defined as the interval between an end-user dispatching a request and the arrival of the corresponding response from the session partner. Minor differences in this definition revolve around the interpretation of when the response has actually arrived.

Availability is the state of a given network facility being functional at a given time. Availability is generally measured as the ratio of the actual functional amount of time to the committed functional amount of time, expressed as a percentage. Availability is the most difficult network attribute to measure because the availability of a given network element is dependent on the availability of other network elements in the path to it. Thus, the availability of a given network element may vary with the point of access to the network.

Efficiency is the quality of meeting service and availability objectives for the minimum cost. Because there are so many differences in the resource requirements, efficiency is generally measured on an application-by-application basis and frequently by user group as well.

NETWORK TOPOLOGY

Network topology is the general name given to the physical layout of network nodes and links most often represented as "ball-and-stick" diagrams on network managers' office walls. As complex as these diagrams often appear at first glance, virtually all networks use one of three basic designs or topologies:

- o Bus
- o Ring
- o Star

The majority of network traffic is routed to or from applications that reside in the network's mainframe processors (host subarea nodes). The communications processor subarea nodes which are channel-attached to these processors and the links which interconnect them are subject to the highest traffic loads and are of the highest concern in network design. These nodes and links together are referred to as the network backbone. Defining the structure of the network backbone in terms of the three basic architectures clarify much of any network structure being examined.

Bus Topology

Bus topologies are the simplest form of network design. Bus structures result when there are only two nodes in the network backbone. In practice this usually results when an organization has two operational centers (one or both of which may have mainframe processors) which are fairly widely separated geographically. Figure 2-9 is a schematic representation of a network employing bus topology.

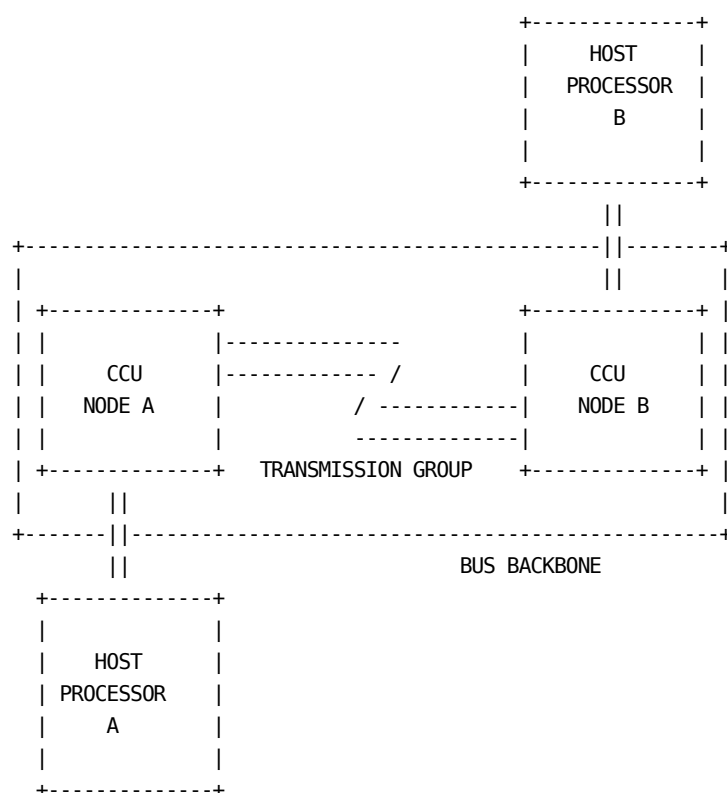


Figure 2-9. Bus Topology

Ring Topology

Ring topologies result when each node in the backbone is connected to two adjacent backbone nodes. This is typically done to reduce the dependence on the availability of an intermediate or "through" node by providing an alternate path. Ring structures are common in organizations with decentralized operational centers. Figure 2-10 is a schematic representation of a network employing ring topology.

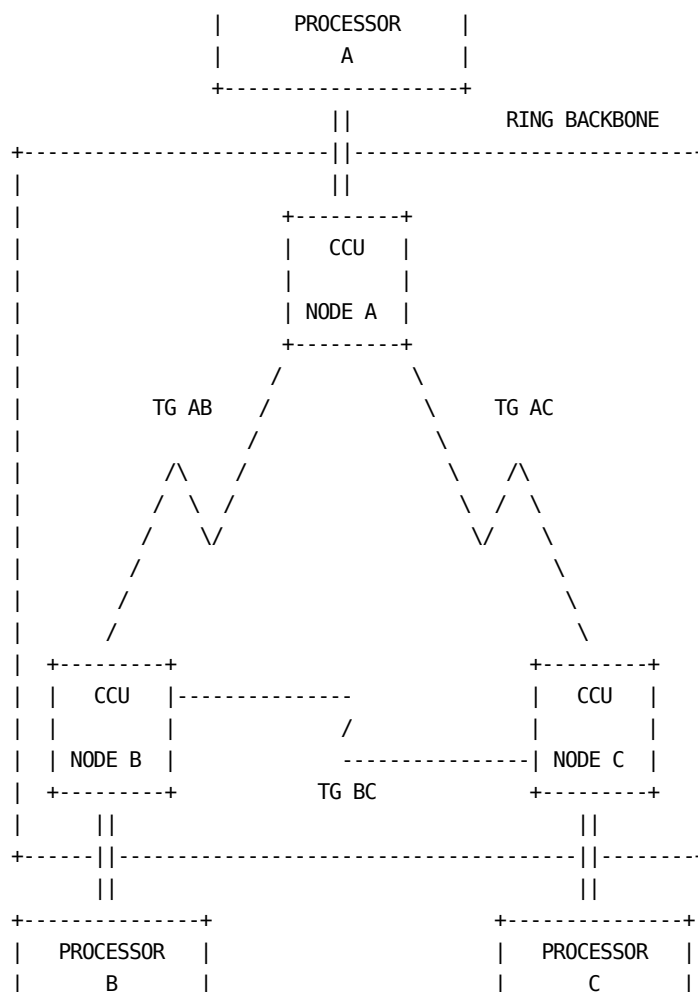


Figure 2-10. Ring Topology

Star Topology

Star topologies are used when the operational centers of an organization are geographically separated but the mainframe processing capabilities are centralized. The star design reduces communications line costs by multiplexing multiple sessions across the transmission group(s) linking the remote node to the central node. Figure 2-11 is a schematic representation of a network employing star topology.

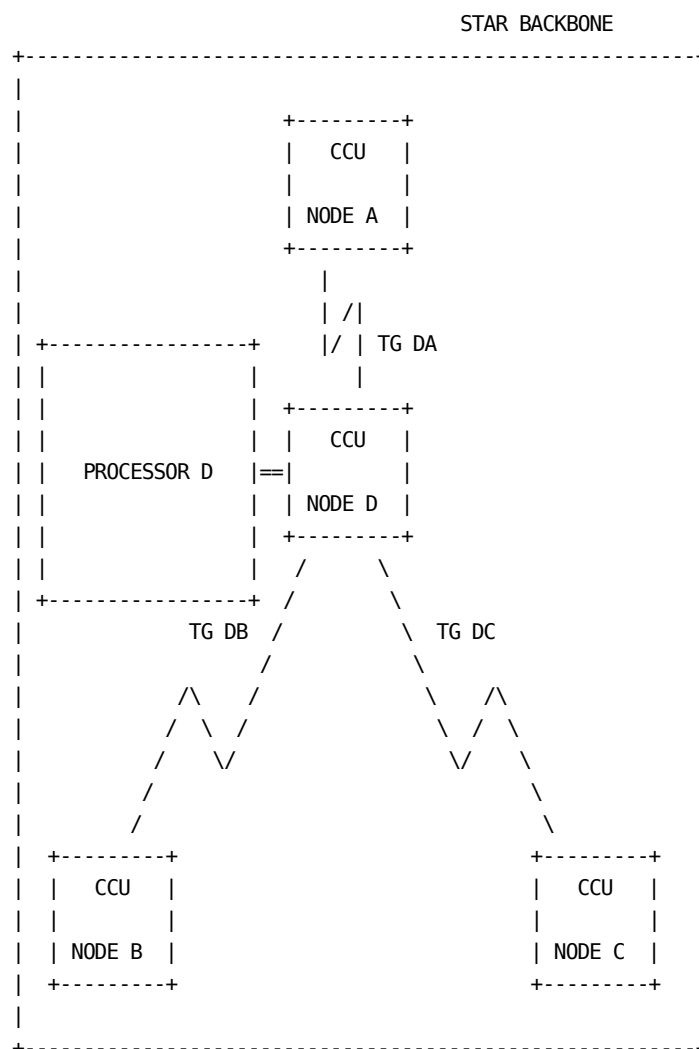


Figure 2-11. Star Topology

While the network backbone is not an SNA concept, it is nonetheless a functional entity. Its utility is twofold: it makes it easier to visualize the network structure and it identifies the nodes and links that are most vital to network performance and availability. Once the backbone structure has been designed, it must be defined using the SNA routing techniques, which are briefly outlined below.

NETWORK LINK CONFIGURATION AND DATA FLOW

SNA network links are organized into several different logical and physical configurations based on the complexity of the network and the type of sessions supported.

Adjacent communications controllers can be connected by multiple links operating concurrently. These are called parallel links. Each parallel link must be assigned to a logical entity called a transmission group (TG). A transmission group appears as a single link to the path control network. Software within the CCU acts to evenly distribute the load across the links which make up a TG.

To allow data to flow in the network, one or more paths must be defined between each pair of network addressable units (NAUs). Paths are defined by specifying an explicit route (ER) and, if necessary, a peripheral link. The explicit route is the portion of the path between two subarea nodes. The peripheral link is the portion of the path between a subarea node and a peripheral node.

Path definitions are distributed among all the nodes along the path and stored in routing tables. A routing table entry exists for each path and consists of the destination node, explicit route number, next subarea node, and applicable transmission group number. Thus each node retains only enough information to route the message to the next node.

Session traffic is assigned to a logical connection called a virtual route. Virtual routes are then mapped to an explicit route. Virtual routes can have up to three different transmission priorities. Messages are queued and selected for transmission on a TG based on these transmission priorities.

Virtual routes are assigned to a session when it is initiated. A session-initiation request contains a class of service. The SSCP looks up this class of service in its class of service table, which contains pairs of virtual routes and transmission priorities, to assign a particular virtual route to the session.

FLOW CONTROL

Because of the relatively autonomous and asynchronous nature of session traffic throughout the network, the amount of data to be sent to a given node at any time may exceed that node's ability to accept data. Since any network element's ability to buffer data is limited, some method of preventing overload is required; this technique is called flow control. SNA flow control is implemented through pacing. Pacing allows a receiving node to limit the rate at which traffic is sent to it. SNA defines two types of pacing:

- o Session-level pacing
- o Virtual-route pacing

Both session-level and virtual-route pacing are based on a pacing window whose size is the number of message units that can be outstanding between origin and destination. When this limit is reached, the sender stops sending until the receiver acknowledges readiness by sending a pacing response.

Specifying explicit routes defines the network topology in an SNA environment. The specification of virtual routes, transmission priorities, and pacing parameters controls service levels and throughput for network services.

2.2.2.3 SNA Session Activation and Termination

Data can only flow in an SNA network when a logical relationship, called a session, has been established. This section discusses the basic requirements for activating and terminating sessions. Logical data management facilities of SNA such as routing and pacing are also outlined.

ACTIVATING NETWORK RESOURCES

One of the major functions of system services control points (SSCPs) is to activate network resources. An SSCP activates SSCP-PU and SSCP-LU sessions with the physical (PU) and logical (LU) units which were defined to it at system generation. These sessions remain active until network deactivation. The SSCP uses the SSCP-PU session to monitor and control the resources in that node. A logical unit requests LU-LU session initiation from the SSCP via the SSCP-LU session.

During network start-up, an SSCP must activate the link to an adjacent node before it can activate SSCP-PU and SSCP-LU sessions with that node. The SSCP sends commands, over the existing SSCP-PU session with the PU at one end of the link, to issue link-level commands to the adjacent link stations which complete the link activation procedure. Because a link must be activated from both ends, the control point in the node at the other end of the link must also request link activation.

INITIATING LU-LU SESSIONS

The purpose of an SNA network is to allow communications between end-users, either individuals or application programs. End-users communicate via an LU-LU session. An LU-LU session is initiated when an LU sends a session-initiation request to its SSCP via the SSCP-LU session. The SSCP performs three functions upon receipt of the request:

- o Verifies that a path is available between the two LUs.
- o Verifies that the LUs are authorized to communicate with each other.
- o Verifies that the LUs can agree on a set of session protocols.

ACTIVATING LU-LU SESSIONS

When the verifications are completed, the SSCP returns a control initiate (CINIT) request to the LU that will activate the session; this LU is designated the primary LU (PLU). This request contains a set of parameters (called the BIND image) that the requesting LU can support.

The PLU uses the BIND image to format a BIND session request which is sent to the secondary logical unit (SLU), its intended session partner. The BIND specifies the protocols that the LU will use when communicating. There are two types of BIND requests: negotiable and non-negotiable.

The SLU can either accept or reject a non-negotiable BIND. If it accepts the parameters, it returns a positive response to the PLU and the session becomes active. In this case the PLU returns a session started request to the SSCP. If the parameters are unacceptable, the SLU returns a negative response thus rejecting the BIND. In this case, the PLU sends a BIND session failure request to the SSCP.

When an SLU receives a negotiable BIND request, it can return an alternate set of parameters to the PLU if the original set is unacceptable. If the alternate parameters are acceptable to the PLU, the session becomes active. In either case, the SSCP is notified of the resolution of the BIND request in the same manner as for non-negotiable BINDs.

TERMINATING LU-LU SESSIONS

An LU-LU session remains active until one of the session partners sends a session-termination request to its SSCP. Only the primary logical unit can actually deactivate a session (except in the case of session between type 6.2 LUs where either the PLU or SLU can terminate the session), but either LU can request session termination.

Usually, the SLU requests session termination by sending a terminate-self (TERM-SELF) request to its SSCP. The SSCP sends a control terminate (CTERM) request to the PLU to notify it that the SLU has requested termination. If the PLU has finished communicating with the SLU, it sends an UNBIND request to the SLU to terminate the session. If the PLU has not finished communicating with the SLU, it ignores the CTERM until it is finished.

When the PLU initiates session termination, it sends a shutdown (SHUTD) request to the SLU. When all outstanding communication has been completed, the SLU returns a shutdown complete (SHUTC) to the PLU. Upon receipt of the SHUTC, the PLU sends an UNBIND request to terminate the session.

Type 6.2 LUs do not use shutdown requests for session termination. Instead, the PLU sends a bracket initiation stopped (BIS) request to the SLU, which returns a BIS reply when all outstanding work is complete. The PLU then sends an UNBIND request to terminate the session.

2.2.3 Comparison of SNA and the OSI Model

SNA is the IBM data communication network architecture. Other organizations and vendors have developed their own architectures. Often, data communications architectures are compared to the generalized structure developed by the International Standards Organization (ISO). The ISO architecture is known as Open Systems Interconnection or OSI. Since the OSI model is commonly referred to, its fundamentals are briefly presented here.

The OSI model consists of seven functional layers organized similarly to the seven SNA layers. Figure 2-12 shows the hierarchical arrangement of the layers in the OSI model.

Confusion sometimes exists due to comparisons between SNA and OSI because, while the structures are similar, the design objectives are different. SNA defines the characteristics required for exchanges among nodes made up of products which conform to a single architecture (i.e., IBM and compatible products). OSI is designed to standardize protocols, thus allowing communications between nodes adhering to dissimilar architectures.

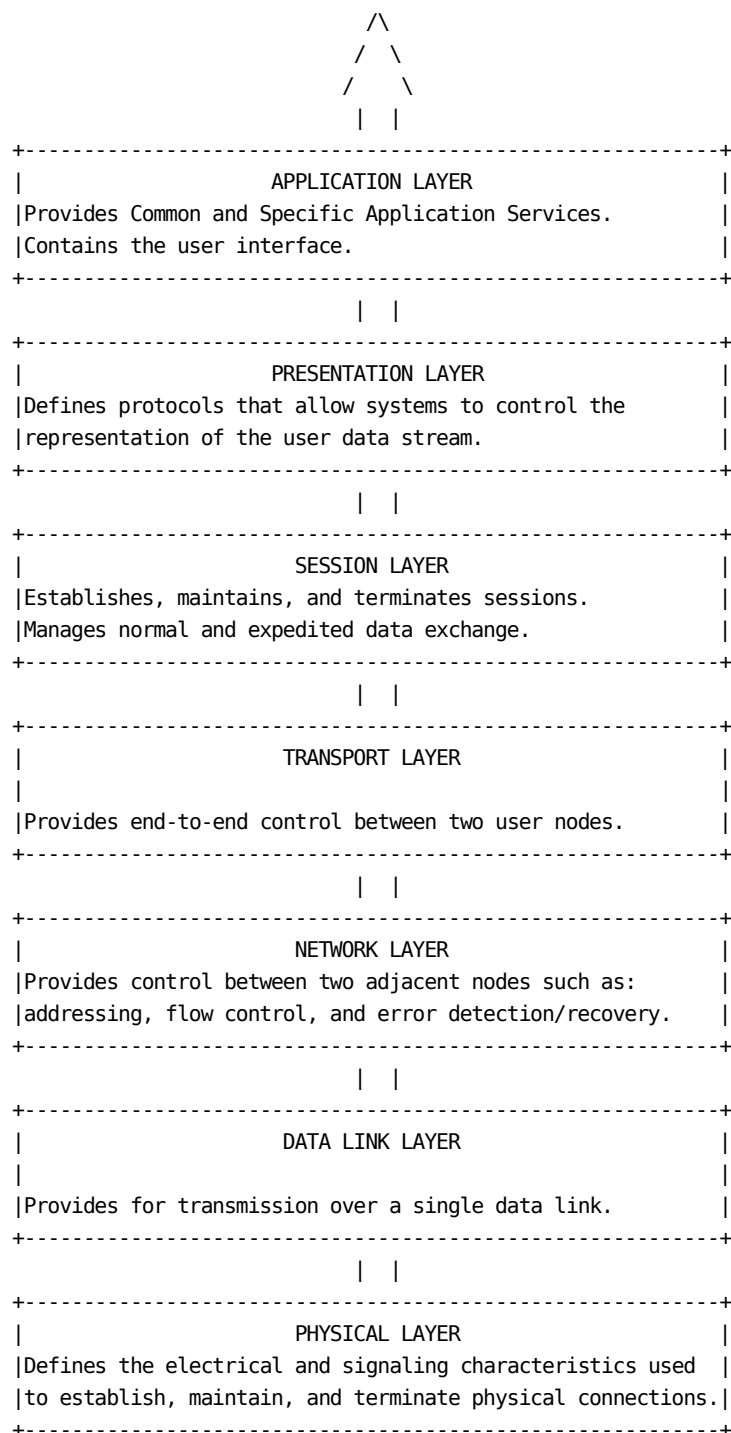


Figure 2-12. The OSI Model

2.2.4 TCP/IP Overview

Transport Communication Protocol/Internet Protocol is a set of industry standard protocols and applications that allow you to share data and computing resources with other computers. By using TCP/IP commands at your workstation, you can perform tasks and communicate easily with a variety of other systems and workstations. TCP/IP allows you to perform tasks independent of the computer types involved in the communication.

The TCP/IP protocols connect equipment from different vendors. It is capable of running over many different types of media and data links. It combines a set of networks into a single network.

TCP/IP provides several common services across multiple platforms. These services are:

- o Electronic Mail (Email)
- o File Transfer
- o Telnet or Remote Logon

The specific structure selected for TCP/IP protocols was dictated by requirements that evolved in academic and defense communities. IP does what is needed to glue different networks into an internet. TCP provides reliable data transfer. In a layered model, IP protocol follows Physical Layer (The physical layer deals with physical media, connectors, and signals that represent 0s and 1s.) and Data Link Layer (At this layer data is organized into units called frames. Each frame has a header that includes address and control information and a trailer that is used for error detection.). IP protocols perform network layer functions. It routes data between systems. TCP layer follows IP layer. It performs transport layer functions. It provides reliable data connection services to applications that were lacking at the IP layer. It contains mechanisms that guarantee that data is delivered error-free, without omission, and in sequence.

2.3 Use Within the Information Structure

The maximum value of data, such as that made available by the CA MICS Network Analyzer, is realized when the data is analyzed and presented within a comprehensive information organization or structure. The organization of this chapter is based on an information structure by which Information Systems (I/S) management can define and classify the various users of information within the I/S group, and understand what information is required for their responsibilities to be effectively managed.

The following sections provide many suggestions, recommended reports, techniques, and other considerations to help you in your analysis and use of the data contained in the CA MICS files. Section 2.3.1 provides an introduction to the concept of an information structure, Section 2.3.2 explains how to locate an area of interest within this section, and the remaining 2.3.x sections provide guidelines and considerations for using and analyzing SNA data.

- 1 - Introduction to the Information Structure
- 2 - Index into the Information Structure
- 3 - Service Level Analysis
- 4 - Installation Environment Analysis

2.3.1 Introduction to the Information Structure

The information structure (Figure 2-13) provides the means for identifying and organizing information about the processes that comprise the business operations of an I/S organization. The information structure is hierarchical and contains three distinct levels:

- o Management Areas

Management areas are at the top level of the structure. Five broad areas of Information Systems (I/S) management concern make up this group: service levels, installation environment, development, administration, and planning.

- o Activity Areas

Activity areas, the second level, consist of the individual activities related to each of the five management areas. For example, under the service level area, there are performance, throughput, availability, and effectiveness activities.

- o Responsibility Areas

Responsibility areas are the third level of the structure, representing detailed subdivisions of the activity areas. By separating activities into areas of common responsibility, these items identify the numerous management responsibilities in a definitive and manageable form. Often, a responsibility area represents a service to the end-user (e.g., TSO Time Sharing Services) or a specific internal I/S management process (e.g., Vendor Contract Administration).

The information structure presented in this guide serves as the method by which a multitude of management indicators are reported for all levels of I/S management, and provides a vital unifying role in establishing a common format for information presentation to all levels of management.

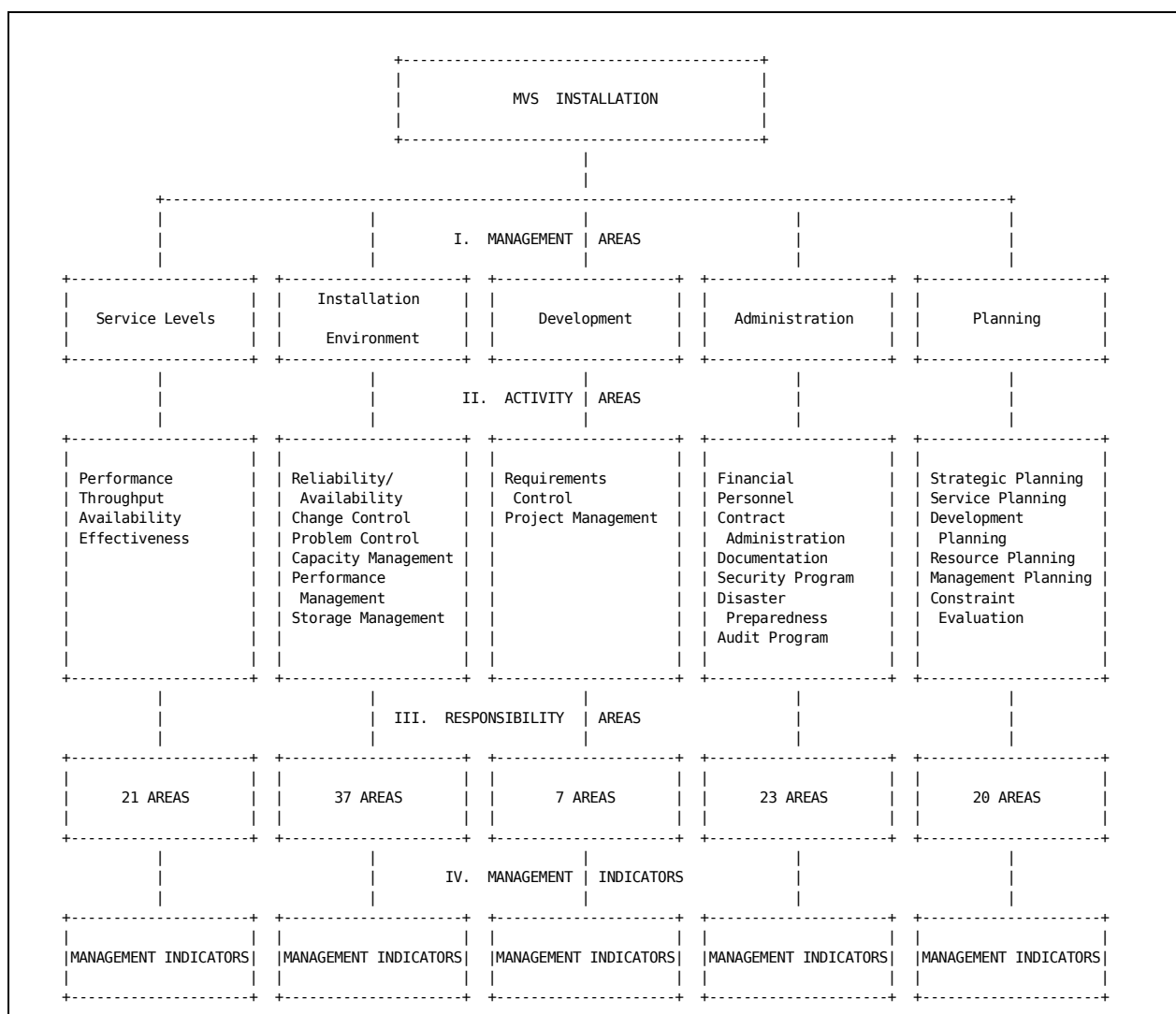


Figure 2-13. Information Structure

2.3.2 Index into the Information Structure

Using the information structure, you can identify the areas of interest and applicable activity, and locate their usage considerations.

The structure is a two-level tier, organized first by management area and then by activity area.

SERVICE LEVELS AREA

The service levels area consists of activities related to the management of service levels (service) and includes those items necessary for providing daily data processing services in the most efficient and effective manner, as well as for meeting service objectives and agreements. The primary activities are the following:

- o Performance
- o Availability
- o Throughput
- o Effectiveness

INSTALLATION ENVIRONMENT AREA

The installation environment area is represented by activities related to operation of the I/S business -- plant management. It includes those items which monitor the I/S production environment in order to maintain operational readiness of hardware, software, network, and facilities. The primary activities are the following:

- o Reliability
- o Problem Control
- o Performance Management
- o Change Control
- o Capacity Management
- o Storage Management

DEVELOPMENT AREA

The development area consists of activities related to the creation, procurement, and modification of applications, hardware, networks, software, management systems, facilities, and other resources used in the information production and distribution processes. The primary activities are the following:

- o Requirements Control
- o Project Management

ADMINISTRATION AREA

The administration area is represented by activities related to the administrative responsibilities and includes security, financial, personnel, education, and training needed to support the total I/S operation. The primary activities are the following:

- o Financial
- o Contracts Administration
- o Security Program
- o Personnel
- o Documentation
- o Disaster Preparedness

PLANNING AREA

The planning area consists of activities involved in setting the direction and the objectives for I/S in terms of what services are to be provided, when they will be provided, and how they will be provided. The primary activities are the following:

- o Strategic Planning
- o Development Planning
- o Management Planning
- o Service Planning
- o Resource Planning
- o Constraint Evaluation

CA MICS provides data and information analysis capabilities in the service level and installation environment areas. Figure 2-14 presents the activity area index for the CA MICS Network Analyzer.

+-----+-----+		
Service Levels Area		
Performance	Section 2.3.3.1	
Throughput	Section 2.3.3.2	
Availability	n/a	
Effectiveness	n/a	
Installation Environment		
Reliability	Section 2.3.4.1	
Change Control	n/a	
Problem Control	n/a	
Capacity Management	Section 2.3.4.2	
Performance Management	Section 2.3.4.3	
Storage Management	n/a	
Development		
Requirements Control	n/a	
Project Management	n/a	

Administration		
Financial	n/a	
Personnel	n/a	
Contracts Administration	n/a	
Documentation	n/a	
Security Program	n/a	
Disaster Preparedness	n/a	
Planning		
Strategic Planning	n/a	
Service Planning	n/a	
Development Planning	n/a	
Resource Planning	n/a	
Management Planning	n/a	
Constraint Evaluation	n/a	
+-----+	+-----+	+-----+

Figure 2-14. Activity Area Index for Network Data

2.3.3 Service Level Analysis

Service level analysis consists of activities related to the management of performance, throughput, availability, and effectiveness in the delivery of communications facilities. The CA MICS Network Analyzer addresses two of these areas as explained in the following sections:

- 1 - Service Levels: Performance
- 2 - Service Levels: Throughput

2.3.3.1 Service Levels: Performance

Network service levels are areas of prime concern to the management of the installation as a whole, and particularly to the network management staff, because service levels measure how efficiently and effectively network facilities are delivered to the end-user. Service levels are best analyzed in relation to an installation-defined set of service level objectives. Service level objectives may be set in different ways based on criteria that are often unique to the installation and depend on its organization, management objectives, and financial considerations. Several types of objective strategies are discussed below.

HOST SERVICE OBJECTIVES

Prior to the availability of end-user response time measurements, host service objectives were the only available management indicators of communications effectiveness. Tivoli's NetView Performance Monitor and CA NetSpy make it possible to measure host response time separately from network response time, thus allowing host response objectives to be retained. The advantage of defining separate host service objectives is that they can identify developing host service problems even when end-user response time is within the overall objectives. Generally, host service objectives are set on an application-by-application basis because each application has different host processing resource requirements.

NETWORK SERVICE OBJECTIVES

Network service objectives define the requirements for delivery of service outboard of the host processor. These objectives are of considerable interest because, until recently, this information was largely unavailable. Network service objectives must be set with regard to network considerations rather than existing host-processor considerations. Two general classifications of network service are reasonable:

- o Topology Based
 - Communications path design constraints
 - Media type constraints
 - . local versus remote

- . link speed
- . multi-drop versus dedicated link
- . satellite versus land line

- o Resource Based

- Class of service as defined by network tuning parameters
- Volume of data transmitted

END-USER (TOTAL) SERVICE OBJECTIVES

In general, total service objectives should be close to the sum of the applicable network and host service objectives for each breakdown of network traffic. Neither Tivoli's NetView Session Monitor nor CA NetMaster NTS measures host and network response time independently. They each allow all of the variations mentioned above to be accommodated through the use of installation-defined performance classes. NetView performance class definitions and CA NetMaster NTS RTM class definitions should be carefully evaluated based on the considerations mentioned above.

The following sections suggest key data elements, exception conditions, component reports, and sample analyses which may be helpful in the management of performance levels:

- 1 - Performance Level Indicators
- 2 - Performance Level Exceptions
- 3 - Performance Level Reports
- 4 - Performance Level Analysis

2.3.3.1.1 Performance Level Indicators

In preparing reports for dissemination to Information Systems and user management, it is important that the measures reported are understandable and pertinent to the subject being reported. The data elements listed below best represent the data elements you may use to report network service levels. These elements are discussed in detail in Appendix B, which contains the Network (SNT) and NetView Session (NVS) Information Areas.

```
+-----+
|  MANAGEMENT AREA:  Service Levels          |
|    ACTIVITY AREA:  Performance              |
|      RESPONSIBILITY AREA:  Network          |
+-----+
```

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTPSU	PSUAVNTM	Average Network Response Time
SNTPSU	PSUAVHTM	Average Host Response Time
SNTPSU	PSUAVTTM	Average Total Response Time
SNTPSU	PSUBRESC	Response Event Count (Both)
SNTPSU	PSUPCBR1	Cum. Pct Both Resp Within Limit 1
SNTPSU	PSUPCBR2	Cum. Pct Both Resp Within Limit 2
SNTPSU	PSUPCBR3	Cum. Pct Both Resp Within Limit 3
SNTPSU	PSUPCBR4	Cum. Pct Both Resp Within Limit 4
SNTPSU	PSUPCHR1	Cum. Pct Host Resp Within Limit 1
SNTPSU	PSUPCHR2	Cum. Pct Host Resp Within Limit 2
SNTPSU	PSUPCHR3	Cum. Pct Host Resp Within Limit 3
SNTPSU	PSUPCHR4	Cum. Pct Host Resp Within Limit 4
SNTPSU	PSUPCTR1	Cum. Pct Total Resp Within Limit 1
SNTPSU	PSUPCTR2	Cum. Pct Total Resp Within Limit 2
SNTPSU	PSUPCTR3	Cum. Pct Total Resp Within Limit 3
SNTPSU	PSUPCNON	Pct of Total Events W/out Netwk Resp
SNTPSU	PSUTDST1	Response Distribution Count 1 (Total)
SNTPSU	PSUTDST2	Response Distribution Count 2 (Total)
SNTPSU	PSUTDST3	Response Distribution Count 3 (Total)
SNTPSU	PSUTDST4	Response Distribution Count 4 (Total)
SNTPSU	PSUTDST5	Response Distribution Count 5 (Total)
SNTPSU	PSUMXHTM	Maximum Host Resp Time
SNTPSU	PSUMXNTM	Maximum Net Resp Time (w/ Host Tx)
SNTPSU	PSUMXTTM	Maximum Total Resp Time
SNTPSU	PSUERQTM	Total Time Exceeded Squared
SNTPSU	PSUERTTM	Total Time Oper Threshold Exceeded
SNTPSU	PSUHRQTM	Host Response Time Squared
SNTPSU	PSUNNHTM	Net Resp Time
SNTPSU	PSUNRNNH	Resp Event Count (Net)
SNTPSU	PSUNRQTM	Net Response Time Squared (w/ Host Tx)

SNTPSU	PSUORQTM	Net Resp Time Squared
SNTPSU	PSUTRQTM	Total Resp Time Squared
SNTPSU	PSUMXNNH	Maximum Net Resp Time

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTPSY	PSYAVNTM	Average Network Response Time
SNTPSY	PSYAVHTM	Average Host Response Time
SNTPSY	PSYAVTTM	Average Total Response Time
SNTPSY	PSYBRES	Response Event Count (Both)
SNTPSY	PSYPCBR1	Cum. Pct Both Resp Within Limit 1
SNTPSY	PSYPCBR2	Cum. Pct Both Resp Within Limit 2
SNTPSY	PSYPCBR3	Cum. Pct Both Resp Within Limit 3
SNTPSY	PSYPCBR4	Cum. Pct Both Resp Within Limit 4
SNTPSY	PSYPCR1	Cum. Pct Host Resp Within Limit 1
SNTPSY	PSYPCR2	Cum. Pct Host Resp Within Limit 2
SNTPSY	PSYPCR3	Cum. Pct Host Resp Within Limit 3
SNTPSY	PSYPCR4	Cum. Pct Host Resp Within Limit 4
SNTPSY	PSYPCTR1	Cum. Pct Total Resp Within Limit 1
SNTPSY	PSYPCTR2	Cum. Pct Total Resp Within Limit 2
SNTPSY	PSYPCTR3	Cum. Pct Total Resp Within Limit 3
SNTPSY	PSYPCNON	Pct of Total Events W/out Netwk Resp
SNTPSY	PSYTDST1	Response Distribution Count 1 (Total)
SNTPSY	PSYTDST2	Response Distribution Count 2 (Total)
SNTPSY	PSYTDST3	Response Distribution Count 3 (Total)
SNTPSY	PSYTDST4	Response Distribution Count 4 (Total)
SNTPSY	PSYTDST5	Response Distribution Count 5 (Total)
SNTPSY	PSYMXHTM	Maximum Host Resp Time
SNTPSY	PSYMXNTM	Maximum Net Resp Time (w/ Host Tx)
SNTPSY	PSYMXTTM	Maximum Total Resp Time
SNTPSY	PSYERQTM	Total Time Exceeded Squared
SNTPSY	PSYERTTM	Total Time Oper Threshold Exceeded
SNTPSY	PSYHRQTM	Host Response Time Squared
SNTPSY	PSYNNHTM	Net Resp Time
SNTPSY	PSYNRHO	Number of Host Only Transactions
SNTPSY	PSYNRNNH	Resp Event Count (Host)
SNTPSY	PSYNRQTM	Net Response Time Squared (w/ Host Tx)
SNTPSY	PSYORQTM	Net Resp Time Squared
SNTPSY	PSYTRQTM	Total Resp Time Squared
SNTPSY	PSYMXNNH	Maximum Net Resp Time

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNPL	NPLAVNTM	Average Network Response Time
SNTNPL	NPLAVHTM	Average Host Response Time
SNTNPL	NPLAVTTM	Average Total Response Time
SNTNPL	NPLBRES	Response Event Count (Both)
SNTNPL	NPLPCBR1	Cum. Pct Both Resp Within Limit 1
SNTNPL	NPLPCBR2	Cum. Pct Both Resp Within Limit 2

SNTNPL	NPLPCBR3	Cum. Pct Both Resp Within Limit 3
SNTNPL	NPLPCBR4	Cum. Pct Both Resp Within Limit 4
SNTNPL	NPLPCHR1	Cum. Pct Host Resp Within Limit 1
SNTNPL	NPLPCHR2	Cum. Pct Host Resp Within Limit 2
SNTNPL	NPLPCHR3	Cum. Pct Host Resp Within Limit 3
SNTNPL	NPLPCHR4	Cum. Pct Host Resp Within Limit 4
SNTNPL	NPLPCTR1	Cum. Pct Total Resp Within Limit 1
SNTNPL	NPLPCTR2	Cum. Pct Total Resp Within Limit 2
SNTNPL	NPLPCTR3	Cum. Pct Total Resp Within Limit 3
SNTNPL	NPLPCNON	Pct of Total Events W/out Netwk Resp
SNTNPL	NPLTDST1	Response Distribution Count 1 (Total)
SNTNPL	NPLTDST2	Response Distribution Count 2 (Total)
SNTNPL	NPLTDST3	Response Distribution Count 3 (Total)
SNTNPL	NPLTDST4	Response Distribution Count 4 (Total)
SNTNPL	NPLTDST5	Response Distribution Count 5 (Total)
SNTNPL	NPLMXHTM	Maximum Host Resp Time
SNTNPL	NPLMXNTM	Maximum Net Resp Time w/ Host Tx
SNTNPL	NPLMXTTM	Maximum Total Resp Time
SNTNPL	NPLERQTM	Total Time Exceeded Squared
SNTNPL	NPLERTTM	Total Time Oper Threshold Exceeded
SNTNPL	NPLHRQTM	Host Response Time Squared
SNTNPL	NPLNNHTM	Net Resp Time
SNTNPL	NPLNRHO	Number of Host Only Transactions
SNTNPL	NPLNRNNH	Resp Event Count (Net)
SNTNPL	NPLNRQTM	Net Response Time Squared (w/ Host Tx)
SNTNPL	NPLORQTM	Net Resp Time Squared
SNTNPL	NPLTRQTM	Total Resp Time Squared
SNTNPL	NPLMXNNH	Maximum Net Resp Time

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNSV	NSVAVTM	Average Total Response Time
SNTNSV	NSVCOS	Class of Service
SNTNSV	NSVPCOBJ	Objective Percentage
SNTNSV	NSVPCOBM	Pct of Times Response Obj Met
SNTNSV	NSVROBTM	Objective Response Time
SNTNSV	NSVTRESC	Total Response Event Count
SNTNSV	NSVPCTR1	Cum. Pct All Response Within Limit 1
SNTNSV	NSVPCTR2	Cum. Pct All Response Within Limit 2
SNTNSV	NSVPCTR3	Cum. Pct All Response Within Limit 3
SNTNSV	NSVPCTR4	Cum. Pct All Response Within Limit 4

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
NVSLSY	LSYAVTM	Average Total Response Time
NVSLSY	LSYCOS	Class of Service
NVSLSY	LSYPCOBJ	Objective Percentage
NVSLSY	LSYPCOBM	Pct of Times Response Obj Met
NVSLSY	LSYROBTM	Objective Response Time

NSVLSY	LSYTRESC	Total Response Event Count
NVSLSY	LSYPCTR1	Cum. Pct All Resp Within Limit 1
NVSLSY	LSYPCTR2	Cum. Pct All Resp Within Limit 2
NVSLSY	LSYPCTR3	Cum. Pct All Resp Within Limit 3
NVSLSY	LSYPCTR4	Cum. Pct All Resp Within Limit 4

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
NVSNLL	NLLAVTTM	Average Total Response Time
NVSNLL	NLLCOS	Class of Service
NVSNLL	NLLPCOBJ	Objective Percentage
NVSNLL	NLLPCOBM	Pct of Times Response Obj Met
NVSNLL	NLLROBTM	Objective Response Time
NSVNLL	NLLTRESC	Total Response Event Count
NVSNLL	NLLPCTR1	Cum. Pct All Resp Within Limit 1
NVSNLL	NLLPCTR2	Cum. Pct All Resp Within Limit 2
NVSNLL	NLLPCTR3	Cum. Pct All Resp Within Limit 3
NVSNLL	NLLPCTR4	Cum. Pct All Resp Within Limit 4

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
NVSRTM	RTMAVTTM	Average Total Response Time
NVSRTM	RTMPCOBJ	Objective Percentage
NVSRTM	RTMPCOBM	Pct of Times Response Obj Met
NVSRTM	RTMROBTM	Objective Response Time
NSVRTM	RTMTRESC	Total Response Event Count
NVSRTM	RTMPCTR1	Cum. Pct All Resp Within Limit 1
NVSRTM	RTMPCTR2	Cum. Pct All Resp Within Limit 2
NVSRTM	RTMPCTR3	Cum. Pct All Resp Within Limit 3
NVSRTM	RTMPCTR4	Cum. Pct All Resp Within Limit 4

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNSP	NSPLHRTM	Last Host Response Time
SNTNSP	NSPLNRTM	Last Network Response Time
SNTNSP	NSPRVAL1	Response Distribution Limit 1
SNTNSP	NSPRVAL2	Response Distribution Limit 2
SNTNSP	NSPRVAL3	Response Distribution Limit 3
SNTNSP	NSPRVAL4	Response Distribution Limit 4
SNTNSP	NSPHRSTM	Host Response Time
SNTNSP	NSPNRESC	Network Responses
SNTNSP	NSPNRSTM	Network Response Time (Measured)
SNTNSP	NSPNRURM	Total User Responses Measured (LU62)
SNTNSP	NSPNRTRI	Number of Transactions (LU62 Sessions)
SNTNSP	NSPRDST1	Response Distribution Count 1
SNTNSP	NSPRDST2	Response Distribution Count 2
SNTNSP	NSPRDST3	Response Distribution Count 3
SNTNSP	NSPRDST4	Response Distribution Count 4
SNTNSP	NSPRDST5	Response Distribution Count 5

SNTNSP	NSPTRESC	Number of Responses
SNTNSP	NSPMXHTM	Maximum Host Response Time
SNTNSP	NSPMXNTM	Maximum Network Response Time
SNTNSP	NSPAVHTM	Average Host Response Time
SNTNSP	NSPAVNTM	Average Network Response Time
SNTNSP	NSPAVTTM	Average Total Response Time
SNTNSP	NSPCNRTM	Network Response Time (Computed)
SNTNSP	NSPPCTR1	Cum. Pct Total Resp Within Limit 1
SNTNSP	NSPPCTR2	Cum. Pct Total Resp Within Limit 2
SNTNSP	NSPPCTR3	Cum. Pct Total Resp Within Limit 3
SNTNSP	NSPPCTR4	Cum. Pct Total Resp Within Limit 4
SNTNSP	NSPTRSTM	Total Response Time

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNSS	NSSLHRTM	Last Host Response Time
SNTNSS	NSSLNRTM	Last Network Response Time
SNTNSS	NSSRVAL1	Response Distribution Limit 1
SNTNSS	NSSRVAL2	Response Distribution Limit 2
SNTNSS	NSSRVAL3	Response Distribution Limit 3
SNTNSS	NSSRVAL4	Response Distribution Limit 4
SNTNSS	NSSHRSTM	Host Response Time
SNTNSS	NSSNRESC	Network Responses
SNTNSS	NSSNRSTM	Network Response Time (Measured)
SNTNSS	NSSNRURM	Total User Responses Measured (LU62)
SNTNSS	NSSNRTRI	Number of Transactions (LU62 Sessions)
SNTNSS	NSSRDST1	Response Distribution Count 1
SNTNSS	NSSRDST2	Response Distribution Count 2
SNTNSS	NSSRDST3	Response Distribution Count 3
SNTNSS	NSSRDST4	Response Distribution Count 4
SNTNSS	NSSRDST5	Response Distribution Count 5
SNTNSS	NSSTRESC	Number of Responses
SNTNSS	NSSMXHTM	Maximum Host Response Time
SNTNSS	NSSMXNTM	Maximum Network Response Time
SNTNSS	NSSAVHTM	Average Host Response Time
SNTNSS	NSSAVNTM	Average Network Response Time
SNTNSS	NSSAVTTM	Average Total Response Time
SNTNSS	NSSCNRTM	Network Response Time (Computed)
SNTNSS	NSSPCTR1	Cum. Pct Total Resp Within Limit 1
SNTNSS	NSSPCTR2	Cum. Pct Total Resp Within Limit 2
SNTNSS	NSSPCTR3	Cum. Pct Total Resp Within Limit 3
SNTNSS	NSSPCTR4	Cum. Pct Total Resp Within Limit 4
SNTNSS	NSSSTRSTM	Total Response Time

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNVR	NVRNRESC	Network Responses (Measured)
SNTNVR	NVRNRSTM	Network Response Time (Measured)
SNTNVR	NVRAVNTM	Average Network Response Time

2.3.3.1.2 Performance Level Exceptions

The following standard exceptions can have applicability when analyzing network performance. These exceptions alert the installation to missed service objectives. The exception reporting provided with the CA MICS Network Analyzer is discussed in Chapter 4 of this guide and detailed descriptions are provided for each of the exceptions.

- o 12301 - Response Objective Missed For Performance Class
- o 12661 - Host Response Outside Bounds-Count Exceeded for SLU
- o 12662 - Net Response Outside Bounds-Count Exceeded for SLU
- o 12663 - Total Response Outside Bounds-Count Exceeded for SLU
- o 12780 - Host Response Outside Bounds-Count Exceeded for Link
- o 12781 - Net Response Outside Bounds-Count Exceeded for Link
- o 12782 - Total Response Outside Bounds-Count Exceeded for Link
- o 12801 - Response Objective Missed for APPL/PCLASS
- o 12802 - Response Objective Missed for LINK/PCLASS
- o 12852 - Invalid Session Parameters Threshold Exceeded
- o 12853 - Virtual Route Inoperative Threshold Exceeded
- o 12854 - Route Extension Inoperative Threshold Exceeded
- o 12855 - Hierarchical Reset Threshold Exceeded
- o 12856 - SSCP Gone Threshold Exceeded
- o 12857 - Virtual Route Deactivated Threshold Exceeded
- o 12858 - LU Failure - Unrecoverable Threshold Exceeded
- o 12859 - LU Failure - Recoverable Threshold Exceeded
- o 12862 - Session Failure Threshold Exceeded

2.3.3.1.3 Performance Level Reports

The standard reports listed below may be useful for analyzing network performance. These reports are described in Chapter 3.

TABULAR REPORTS

- o SNT101 - NPM Service by Application Report
- o SNT103 - NPM Service by Link Report
- o SNT105 - NLDM Service by Performance Class Report
- o SNT111 - NLDM Service by Application
- o SNT112 - NLDM Service by Link
- o SNT113 - NLDM Service by Control Unit
- o SNT114 - NLDM Service by Terminal
- o SNT121 - CA NetSpy Service by Application
- o SNT122 - CA NetSpy Service by Terminal
- o SNT403 - NPM Session Data Collection Report

GRAPHIC INQUIRIES

- o SNTG101 - Average Response by Performance Class
- o SNTG102 - Application Service Analysis
- o SNTG103 - Application Service Analysis by Hour
- o SNTG104 - Response Objective Results by Performance Class

MICF INQUIRIES

- o SNTCD1 - NetView Daily Avg Resp by PCLASS
- o SNTCD4 - NetView Daily % Resp Within Obj. by PCLASS
- o SNTCDI - NetView Daily Avg Response by Link
- o SNTCDN - NetView Daily % Resp Within Obj. by Link
- o SNTCDS - CA NetSpy Daily PLU Resp Time Components
- o SNTCDT - CA NetSpy Daily SLU Resp Time Components
- o SNTLDA - NetView Application Service/Workload Ranking
- o SNTLD0 - NPM Application Service/Workload Ranking
- o SNTLD2 - CA NetSpy Application Service/Workload Ranking

Note that any report listed above that begins with the name of the data source NetView NLDM can also be produced from equivalent data collected by CA NetMaster NTS. Any report beginning with the name of the data source NetView NPDA can also be produced from equivalent data collected by CA NetMaster NEWS.

2.3.3.1.4 Performance Level Analysis

REPORTING RESPONSE TIME DIFFERENCES FOR VIRTUAL ROUTES

While the nodes in the network are physically connected by real links known as explicit routes, network traffic flows over logical connections called virtual routes. These virtual routes assume the physical characteristics (media type, reliability, bandwidth, etc.) of the underlying explicit routes to which they are assigned, but the path control network schedules message units on a virtual route based on its transmission priority.

When a logical unit to logical unit (LU-LU) session is established, the session-initiation request identifies a desired class of service. The system services control point (SSCP) looks-up this class of service in the class of service (COS) table. The COS table lists virtual route and transmission priority pairs. Using the table entry for the requested class of service, the SSCP assigns a virtual route and transmission priority for the session.

Since the virtual routes and transmission priorities are the primary means the network analyst has to regulate traffic flow through the network, knowledge of the service provided to the end-users communicating over a particular virtual route at a specific priority is extremely valuable when maintaining the class of service table. This information is available in the CA MICS Network Analyzer's NLDM Service File by summarizing DETAIL data from the SNTNSV File by virtual route and transmission priority as follows:

```
%INCLUDE INCLLIB(%SNTMACS);
MACRO _BY NSVVRTE NSVTRPTY %
MACRO _BREAK NSVTRPTY %
PROC SORT DATA=_dSNTX.SNTNSV01 OUT=VRSERV; BY _BY;
RUN;

DATA VRSERV; SET VRSERV; BY _BY;
      _NSVSUM
RUN;

PROC PRINT LABELS;
ID NSVVRTE;
VAR NSVTRPTY NSVAVTTM NSVPCTR1 NSVPCTR2 NSVPCTR3
      NSVPCTR4 NSVPCOBM;
RUN;
```

By determining the actual effect of specifying different

transmission priorities for different virtual routes, the class of service table can be made to reflect the organization's business needs more accurately.

2.3.3.2 Service Levels: Throughput

Throughput constraints and capabilities are of primary concern to the network analyst. As in mainframe capacity planning, the network analyst must consider the various workloads that affect the data center. Workload can conveniently be divided into two broad classes: logical workloads and physical workloads.

LOGICAL WORKLOADS

Logical workloads are directly related to the end user. Planning for new systems or major configuration changes is usually concerned initially with logical workloads. Logical workloads can be subdivided into two categories: application workloads and organization (business) unit workloads.

Application workloads are identified in the following files:

- o SNTPSY - NPM System Activity File
- o NVLSY - NLDM System Activity File
- o SNTNSP - CA NetSpy Application File

Organizational unit workloads can be identified via the use of account code data elements in the following files:

- o NCP Network Accounting (SNTNAC) File
- o CA NetSpy Terminal (SNTNSS) File
- o NPM User Activity (SNTPSU) File
- o NLDM Session Accounting (NVSNSA) File
- o NLDM Session Connectivity (NVSNSC) File
- o NLDM Response Time (NVSRTM) File
- o NLDM Route (NVS RTE) File

Sample account code definition members are included with this product, and the use of account codes is discussed in Section 7.2. However, it is your responsibility to verify that the account code structure meets the requirements of your data center, and, if not, to make any necessary modifications. In this way, you are assured the greatest flexibility in defining an account code structure that will satisfy your network analysis and reporting requirements.

PHYSICAL WORKLOADS

Physical workloads are directly related to network topology

and may only incidentally be related to the end user. Localized network performance considerations such as load balancing and NCP parameter selection are most often concerned with physical workloads. Physical workloads can be divided into two categories: boundary workloads and backbone workloads.

The sequence/summary variable SLULINK in the NPM Link Activity (SNTNPL) File and the NLDM Link Activity (NVSNLL) File contains the name of the peripheral link to which the secondary logical unit's physical unit is attached. Network boundary (peripheral link) workloads may thus be identified directly. Coincidentally, they may also be identified in the CA NetSpy Terminal (SNTNSS) File, and in the NLDM Service (SNTNSV) and the NLDM System Activity (NVSLSY) Files, depending on the definition of performance classes for NetView/NLDM and RTM classes for CA NetMaster NTS.

Performance problems related to boundary workloads are limited in scope because they are localized to a specific peripheral link. However, if the link attaches a distributed processor, a significant number of end users may be affected.

Backbone workloads may be identified by summarizing utilization data to the level of the primary and secondary logical unit's subareas (note that the CA MICS summarization facility, explained in the CA MICS Standard Reporting Guide, should always be utilized for any summarization of CA MICS files). This yields the traffic load between subarea "x" and subarea "y".

If you are processing CA NetSpy Virtual Route Activity data, you will find information about both SNA backbone virtual route traffic volumes and response times in the CA NetSpy Virtual Route Activity (SNTNVR) File.

Performance problems related to backbone workload constraints can have far-reaching effects in the network and should be closely tracked. Relatively small changes in the traffic mix (message lengths, chaining characteristics, etc.) can cause significant increases in the utilization level of the backbone communications control units.

The following sections suggest key data elements, exception conditions, reports, and sample analysis that may be helpful in the management of network throughput levels:

- 1 - Throughput Level Indicators
- 2 - Throughput Level Exceptions

- 3 - Throughput Level Reports
- 4 - Throughput Level Analysis

2.3.3.2.1 Throughput Level Indicators

In preparing reports for dissemination to Information Systems and user management, it is important that the measures reported are understandable and pertinent to the subject being reported. The data elements listed below best represent the data elements you may use to report network service levels. These elements are discussed in detail in Appendix B, which contains the Network (SNT) and the NetView Session (NVS) Information Areas.

```
-----  
|  MANAGEMENT AREA:  Service Levels  |  
|    ACTIVITY AREA:  Throughput      |  
|    RESPONSIBILITY AREA:  Network   |  
-----
```

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNCL	NCLNRRLS	Receiving Link Speed
SNTNCL	NCLNRSLS	Sending Link Speed
SNTNCL	NCLNRCHR	Number of Bytes Received
SNTNCL	NCLNRCHS	Number of Bytes Sent
SNTNCL	NCLNRIFR	Number of I-Frames Received
SNTNCL	NCLNRIFS	Number of I-Frames Sent
SNTNCL	NCLNRMSR	Number of Messages Received
SNTNCL	NCLNRMSS	Number of Messages Sent
SNTNCL	NCLNRERR	Error Count
SNTNCL	NCLNRRBY	Retransmit Byte Count
SNTNCL	NCLNRRIF	Retransmit I-Frame Count
SNTNCL	NCLNRROQ	Resource Outbound Queue Length
SNTNCL	NCLNRRRR	Total RNR Frames Received
SNTNCL	NCLNRRRS	Total RNR Frames Sent
SNTNCL	NCLNRRFR	Total RR Frames Received
SNTNCL	NCLNRRFS	Total RR Frames Sent
SNTNCL	NCLNRRFD	Number of Receive Frames Discarded
SNTNCL	NCLNRRFM	Number of Receive Frames Misaddressed
SNTNCL	NCLNRRFU	Number of Receive Frames Unrecognized
SNTNCL	NCLMXROQ	Max. Resource Outbound Queue Length
SNTNCL	NCLPCELB	Percent Link Busy Retransmission
SNTNCL	NCLPCLBS	Percent Link Busy
SNTNCL	NCLMXLBS	Max. Percent Link Busy
SNTNCL	NCLMNLBS	Min. Percent Link Busy
SNTNCL	NCLPCRLB	Percent Link Busy Receiving
SNTNCL	NCLMXRLB	Max. Percent Link Busy Receiving
SNTNCL	NCLMNLB	Min. Percent Link Busy Receiving
SNTNCL	NCLPCSLB	Percent Link Busy Sending
SNTNCL	NCLMXSLB	Max. Percent Link Busy Sending
SNTNCL	NCLMNSLB	Min. Percent Link Busy Sending

SNTNCL	NCLPMCHR	Number of Bytes Received per Minute
SNTNCL	NCLPMCHS	Number of Bytes Sent per Minute
SNTNCL	NCLPMIFR	Number of I-Frames Received per Minute
SNTNCL	NCLPMIFS	Number of I-Frames Sent per Minute
SNTNCL	NCLPMMSR	Number of Messages Received per Minute
SNTNCL	NCLPMMS	Number of Messages Sent per Minute
SNTNCL	NCLPMTPL	Number of Total Polls per Minute

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTCAF	CAFNRRLS	Receiving Link Speed
SNTCAF	CAFNRSLs	Sending Link Speed
SNTCAF	CAFNRCHR	Number of Bytes Received
SNTCAF	CAFNRCHS	Number of Bytes Sent
SNTCAF	CAFNRMSR	Number of Messages Received
SNTCAF	CAFNRPKS	Number of Packets Sent
SNTCAF	CAFNRPKR	Number of Packets Received
SNTCAF	CAFNRMS	Number of Messages Sent
SNTCAF	CAFNRERR	Error Count
SNTCAF	CAFNRBY	Retransmit Byte Count
SNTCAF	CAFNRROQ	Resource Outbound Queue Length
SNTCAF	CAFNRIFS	Number of I-Frames Sent
SNTCAF	CAFNRIFR	Number of I-Frames Received
SNTCAF	CAFNRRI	Retransmitted I-Frame Count
SNTCAF	CAFNRFRS	Number of Frames Sent
SNTCAF	CAFNRFR	Number of Frames Received
SNTCAF	CAFNRRT0	Reply Timeouts
SNTCAF	CAFNRLB0	Local Busy Occurrences
SNTCAF	CAFNRSFS	Rejected Supervisor Frames Sent
SNTCAF	CAFNRSFR	Rejected Supervisor Frames Received
SNTCAF	CAFMRROQ	Max. Resource Outbound Queue Length
SNTCAF	CAFPMCHR	Number of Bytes Received per Minute
SNTCAF	CAFPMCHS	Number of Bytes Sent per Minute
SNTCAF	CAFPMMSR	Number of Messages Received per Minute
SNTCAF	CAFPMMS	Number of Messages Sent per Minute
SNTCAF	CAFMPPKS	Number of Packets Sent per Minute
SNTCAF	CAFMPPKR	Number of Packets Received per Minute
SNTCAF	CAFPMTP	Number of Total Polls per Minute

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTPSU	PSUBRESC	Response Event Count (Both)
SNTPSU	PSUNRFMR	Number Text Bytes Received
SNTPSU	PSUNRFMS	Number Text Bytes Sent
SNTPSU	PSUNRNFR	Number Control Bytes Received
SNTPSU	PSUNRMFS	Number Control Bytes Sent
SNTPSU	PSUNRPFR	Number Text PIUs Received
SNTPSU	PSUNRPFS	Number Text PIUs Sent
SNTPSU	PSUNRPNR	Number Control PIUs Received

SNTPSU	PSUNRPNS	Number Control PIUs Sent
SNTPSU	PSUNRMBR	No. of Text Message Bytes Rec'd
SNTPSU	PSUNRMBS	No. of Text Message Bytes Sent
SNTPSU	PSUNRMSR	No. of Text Messages Rec'd
SNTPSU	PSUNRMSS	No. of Text Messages Sent
SNTPSU	PSUMXMBR	Max Text Message Rec'd
SNTPSU	PSUMXMBS	Max Text Message Sent
SNTPSU	PSUMXTBR	Max Text PIU Rec'd
SNTPSU	PSUMXTBS	Max Text PIU Sent

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTPSY	PSYBRES	Response Event Count (Both)
SNTPSY	PSYNRFMR	Number Text Bytes Received
SNTPSY	PSYNRFMS	Number Text Bytes Sent
SNTPSY	PSYNRNFR	Number Control Bytes Received
SNTPSY	PSYNRMFS	Number Control Bytes Sent
SNTPSY	PSYNRPFR	Number Text PIUs Received
SNTPSY	PSYNRPFS	Number Text PIUs Sent
SNTPSY	PSYNRPNR	Number Control PIUs Received
SNTPSY	PSYNRPNS	Number Control PIUs Sent
SNTPSY	PSYNRMBR	No. of Text Message Bytes Rec'd
SNTPSY	PSYNRMBS	No. of Text Message Bytes Sent
SNTPSY	PSYNRMSR	No. of Text Messages Rec'd
SNTPSY	PSYNRMSS	No. of Text Messages Sent
SNTPSY	PSYMXMBR	Max Text Message Rec'd
SNTPSY	PSYXMBS	Max Text Message Sent
SNTPSY	PSYMXTBR	Max Text PIU Rec'd
SNTPSY	PSYMXTBS	Max Text PIU Sent

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNPL	NPLBRES	Response Event Count (Both)
SNTNPL	NPLNRFMR	Number Text Bytes Received
SNTNPL	NPLNRFMS	Number Text Bytes Sent
SNTNPL	NPLNRNFR	Number Control Bytes Received
SNTNPL	NPLNRMFS	Number Control Bytes Sent
SNTNPL	NPLNRPFR	Number Text PIUs Received
SNTNPL	NPLNRPFS	Number Text PIUs Sent
SNTNPL	NPLNRPNR	Number Control PIUs Received
SNTNPL	NPLNRPNS	Number Control PIUs Sent
SNTNPL	NPLNRMBS	No. of Text Message Bytes Rec'd
SNTNPL	NPLNRMBS	No. of Message Message Bytes Sent
SNTNPL	NPLNRMBS	No. of Text Messages Rec'd
SNTNPL	NPLNRMSS	No. of Text Messages Sent
SNTNPL	NPLMXMBR	Max Text Message Rec'd
SNTNPL	NPLMXMBS	Max Text Message Sent
SNTNPL	NPLMXTBR	Max Text PIU Rec'd
SNTNPL	NPLMXTBS	Max Text PIU Sent

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
NVSLSY	LSYNRCBR	Number Control Bytes Received
NVSLSY	LSYNRCBS	Number Control Bytes Sent
NVSLSY	LSYNRCPR	Number Control PIUs Received
NVSLSY	LSYNRCPS	Number Control PIUs Sent
NVSLSY	LSYNRTBR	Number Text Bytes Received
NVSLSY	LSYNRTBS	Number Text Bytes Sent
NVSLSY	LSYNRTPR	Number Text PIUs Received
NVSLSY	LSYNRTPS	Number Text PIUs Sent
NVSLSY	LSYTRESC	Response Event Count
FILE	ELEMENT	DESCRIPTION
-----	-----	-----
NVSNLL	NLLNRCBR	Number Control Bytes Received
NVSNLL	NLLNRCBS	Number Control Bytes Sent
NVSNLL	NLLNRCPR	Number Control PIUs Received
NVSNLL	NLLNRCPS	Number Control PIUs Sent
NVSNLL	NLLNRTBR	Number Text Bytes Received
NVSNLL	NLLNRTBS	Number Text Bytes Sent
NVSNLL	NLLNRTPR	Number Text PIUs Received
NVSNLL	NLLNRTPS	Number Text PIUs Sent
NVSNLL	NLLTRESC	Response Event Count
FILE	ELEMENT	DESCRIPTION
-----	-----	-----
NVNSA	NSANRCBR	Number Control Bytes Received
NVNSA	NSANRCBS	Number Control Bytes Sent
NVNSA	NSANRCPR	Number Control PIUs Received
NVNSA	NSANRCPS	Number Control PIUs Sent
NVNSA	NSANRTBR	Number Text Bytes Received
NVNSA	NSANRTBS	Number Text Bytes Sent
NVNSA	NSANRTBY	Total Number of Bytes Transmitted
NVNSA	NSANRTPI	Total Number of PIUs Transmitted
NVNSA	NSANRTPR	Number Text PIUs Received
NVNSA	NSANRTPS	Number Text PIUs Sent
FILE	ELEMENT	DESCRIPTION
-----	-----	-----
NVNSC	NSCRTCH	Total Characters Transmitted
FILE	ELEMENT	DESCRIPTION
-----	-----	-----
NVSRTE	RTENRTCH	Total Characters Transmitted
FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNSP	NSPNRBYR	Cumulative Bytes Received

SNTNSP	NSPNRBYS	Cumulative Bytes Sent
SNTNSP	NSPNRESC	Network Responses
SNTNSP	NSPNROUT	Number of Outputs
SNTNSP	NSPNRTRI	Number of Transactions (LU62 Sessions)
SNTNSP	NSPTRESC	Number of Transactions (# of Inputs)

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNSS	NSSNRBYR	Cumulative Bytes Received
SNTNSS	NSSNRBYS	Cumulative Bytes Sent
SNTNSS	NSSNRBYT	Cumulative Bytes Transmitted
SNTNSS	NSSNRESC	Network Responses
SNTNSS	NSSNROUT	Number of Outputs
SNTNSS	NSSNRTRI	Number of Transactions (LU62 Sessions)
SNTNSS	NSSTRESC	Number of Transactions (# of Inputs)

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNVR	NVRNRBYS	Cumulative Bytes Sent
SNTNVR	NVRNRMOP	Measured Outbound PIUs
SNTNVR	NVRNRTOP	Total Outbound PIUs
SNTNVR	NVRAVPL	Average Outbound PIU Length
SNTNVR	NVRNRESC	Network Responses (Measured)

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNAC	NACNRCBR	Number Control Bytes Received
SNTNAC	NACNRCBS	Number Control Bytes Sent
SNTNAC	NACNRCPR	Number Control PIUs Received
SNTNAC	NACNRCPS	Number Control PIUs Sent
SNTNAC	NACNRTBR	Number Text Bytes Received
SNTNAC	NACNRTBS	Number Text Bytes Sent
SNTNAC	NACNRTBY	Total Number of Bytes Transmitted
SNTNAC	NACNRTPI	Total Number of PIUs Transmitted
SNTNAC	NACNRTPR	Number Text PIUs Received
SNTNAC	NACNRTPS	Number Text PIUs Sent

2.3.3.2.2 Throughput Level Exceptions

The standard exceptions listed below may have applicability when analyzing network throughput. These exceptions indicate that throughput thresholds were exceeded. The exception reporting provided with the CA MICS Network Analyzer is discussed in Chapter 4. Detail descriptions are provided for each of the exceptions.

- o 12001 - Link Average Utilization Threshold Exceeded
- o 12002 - Link Error Count Threshold Exceeded
- o 12003 - Link Resource Outbound Queue Length Exceeded
- o 12061 - Network Component Error Threshold Exceeded
- o 12124 - Avg NCP Channel Hold Q Length Threshold Exceeded
- o 12181 - Network Component Traffic Exceeds Limit
- o 12182 - Network Component Traffic Below Minimum
- o 12183 - Network Component Error Rate Exceeds Limit
- o 12184 - NCP Processor Overloaded
- o 12185 - NCP Processor Underutilized
- o 12188 - Messages Per Minute Exceeds Limit
- o 12189 - Bytes Per Second Exceeds Limit
- o 12193 - Percentage of Bytes Retransmitted Exceeds Limit
- o 12194 - Percentage of NCP Buffers Used Exceeds Limit

2.3.3.2.3 Throughput Level Reports

The standard reports listed below may be applicable when analyzing network throughput. These reports are described in Chapter 3.

TABULAR REPORTS

- o SNT201 - NPM Workload by Application Report
- o SNT203 - NPM Workload by Link Report
- o SNT208 - NPM/NetSpy Utilization by NCP Report
- o SNT209 - NPM/NetSpy NCP Workload by Link Report
- o SNT211 - NLDM Workload by Application
- o SNT212 - NLDM Workload by Link
- o SNT213 - NLDM Workload by Control Unit
- o SNT214 - NLDM Workload by Terminal
- o SNT215 - NPM/NetSpy NCP Workload by Link Report
- o SNT216 - NPM/NetSpy NCP Workload by Link Report
- o SNT221 - CA NetSpy Workload by Application
- o SNT222 - CA NetSpy Workload by Terminal
- o SNT401 - NPM NCP Data Collection Report
- o SNT401 - CA NetSpy NCP Data Collection Report
- o SNT403 - NPM Session Data Collection Report

GRAPHIC INQUIRIES

- o SNTG201 - Traffic Profile Report for Link
- o SNTG204 - Percent Link Utilization by Zone

MICF INQUIRIES

- o SNTCD6 - NPM Daily Pct. NCP Cycle Util.
- o SNTCD7 - NPM Daily NCP Buffer Utilization
- o SNTCD8 - NPM Daily Link Utilization
- o SNTCDP - CA NetSpy Daily Pct. NCP Cycle Util.
- o SNTCDQ - CA NetSpy Daily NCP Buffer Utilization
- o SNTCDR - CA NetSpy Daily Link Utilization
- o SNTCDC - NetView Daily Connect Time By SNTACT1
- o SNTCDD - NetView Daily Chars/1000 By SNTACT1
- o SNTCDE - NetView Daily Chars/1000 By VR
- o SNTCDF - NetView Daily Data Chars/1000 By SNTACT1
- o SNTCDG - NetView Daily Cntl Chars/1000 By SNTACT1
- o SNTCWH - NetView Weekly Cntl PIU Traffic By PLU
- o SNTCWK - NetView Weekly Data PIU Traffic By PLU
- o SNTLD4 - NPM Link Service/Workload Ranking
- o SNTLD8 - NetView Link Service/Workload Ranking
- o SNTLDE - NCP Utilization Ranking
- o SNTPDU - NCP Utilization Chart
- o SNTPDV - NCP Utilization Plot

- o SNTCDX - NSA/NGA Daily Chars/1000 By SNTACT1
- o SNTCDY - NSA/NGA Daily PIU Traffic By SNTACT1

Note that any report listed above that begins with the name of the data source NetView NLDM can also be produced from equivalent data collected by CA NetMaster NTS. Any report beginning with the name of the data source NetView NPDA can also be produced from equivalent data collected by CA NetMaster NEWS.

2.3.3.2.4 Throughput Level Analysis

CALCULATING THE AMOUNT OF CROSS-DOMAIN TRAFFIC

Sometimes the network analyst is faced with the question of which of the network's host processors is the optimum location for a given application. If users in several domains have access to the application, it is advantageous to have the application reside in the domain which generates the greatest load. With a new application, this location is often obvious. But, when an application has been widely used over a long period of time, some analysis may be necessary to determine which domain produces the most transactions. This analysis can be accomplished fairly easily using the data in the DETAIL timespan cycles of the NLDM Service (SNTNSV) File as follows:

1. Summarize the data to the PLU, PLDOMAIN and SLDOMAIN

```
%INCLUDE INCLLIB(#SNTMACS);
MACRO _BY PLU PLDOMAIN SLDOMAIN %
MACRO _BREAK SLDOMAIN %
PROC SORT DATA=_dSNTX.SNTNSV01 OUT=DOMAINS; BY _BY;
RUN;

DATA DOMAINS; SET DOMAINS; BY _BY;
      _NSVSUM
RUN;
```

2. Report the total response event count (NSVTRESC) by secondary logical unit domain (SLDOMAIN)

```
PROC PRINT LABELS DATA=DOMAINS; BY PLU;
ID PLUDOMAIN;
VAR SLDOMAIN NSVAVTTM NSVPCOBM;
```

2.3.4 Installation Environment Analysis

Installation environment analysis consists of activities related to the operation of the communications network. These include reliability, change control, problem control, capacity management, performance management, and storage management. The CA MICS Network Analyzer addresses three of these areas as explained in the following sections:

- 1 - Environment: Reliability
- 2 - Environment: Capacity Management
- 3 - Environment: Performance Management

2.3.4.1 Environment: Reliability

The reliability information retained by the CA MICS Network Analyzer is written to SMF by Tivoli NetView Hardware Monitor/NPDA and NPM, CA NetMaster NEWS, and CA NetSpy. The NetView Hardware Monitor and CA NetMaster NEWS reliability data consists of statistics, events, and alerts. Statistics are temporary errors and traffic data. Events include permanent errors and statistics whose error-to-traffic ratios exceed installation-defined thresholds. Alerts are any conditions that require immediate operator attention. NetView Hardware Monitor/NPDA and CA NetMaster recording filters determine which network occurrences are classified as events or alerts. The reliability information from NPM network data and CA NetSpy NCP interface data consists of counts for network errors (e.g., time-out-to-poll), and the number of characters and PIUs that are retransmitted by the NCP.

Be aware that reliability information is NOT availability information. While permanent errors resulting in outages of many of the hardware and software components of the network are recorded in the SNTNEF File, there is no corresponding notation of normal activation or deactivation. Thus, availability reporting can be done only by accessing information, such as network logs, which are outside the scope of the CA MICS Network.

The following sections suggest key data elements, exception conditions, reports, and sample analysis which may be helpful in the management of reliability:

- 1 - Reliability Indicators
- 2 - Reliability Exceptions
- 3 - Reliability Reports
- 4 - Reliability Analysis

2.3.4.1.1 Reliability Indicators

In preparing reports for dissemination to Information Systems and user management, it is important that the measures reported are understandable and pertinent to the subject being reported. The data elements listed below best represent the data elements you may use to report network service levels. These elements are discussed in detail in Appendix B, which contains the Network (SNT) and the NetView Session (NVS) Information Areas.

```

-----
| MANAGEMENT AREA: Environment |
| ACTIVITY AREA: Reliability    |
| RESPONSIBILITY AREA: Network  |
|-----|

```

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNCL	NCLNRERR	Error Count
SNTNCL	NCLNRRBY	Retransmit Byte Count
SNTNCL	NCLNRRIF	Retransmit I-Frame Count
SNTNCL	NCLNRPIU	Retransmit PIU Count
SNTNCL	NCLNRRRR	Total RNR Frames Received
SNTNCL	NCLNRRRS	Total RNR Frames Sent
SNTNCL	NCLNRRFD	Number of Receive Frames Discarded
SNTNCL	NCLNRRFM	Number of Receive Frames Misaddressed
SNTNCL	NCLNRRFU	Number of Receive Frames Unrecognized
SNTNCL	NCLPCELB	Percent Link Busy Retransmission

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTCAF	CAFNRERR	Error Count
SNTCAF	CAFNRRBY	Retransmit Byte Count
SNTCAF	CAFNRPIU	Retransmit PIU Count
SNTCAF	CAFNRRRR	Total RNR Frames Received
SNTCAF	CAFNRRRS	Total RNR Frames Sent
SNTCAF	CAFNRIFS	Number of I-Frames Sent
SNTCAF	CAFNRIFR	Number of I-Frames Received
SNTCAF	CAFNRRIF	Retransmitted I-Frame Count
SNTCAF	CAFNRRT0	Reply Timeouts
SNTCAF	CAFNRLB0	Local Busy Occurrences
SNTCAF	CAFNRSFS	Rejected Supervisor Frames Sent
SNTCAF	CAFNRSFR	Rejected Supervisor Frames Received

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNEF	NEFFRNAME	Failing Resource Name
SNTNEF	NEFFRTYP	Failing Resource Type

SNTNEF	NEFERRDS	Error Description: Probable Cause
SNTNEF	NEFNRLT	Number of Alerts
SNTNEF	NEFNREVT	Number of Events

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNSF	NSFFRNAM	Failing Resource Name
SNTNSF	NSFFRTYP	Failing Resource Type
SNTNSF	NSFERRDS	Error Description: Probable Cause
SNTNSF	NSFNRLT	Number of Alerts
SNTNSF	NSFTTERR	Total Temporary Errors
SNTNSF	NSFPCERR	Pct of Total Traffic w/Temp Errors
SNTNSF	NSFTTRFC	Total Traffic

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
NVSVBF	VBFCause	BIND Failure/UNBIND Reason
NVSVBF	VBFFTYPE	VTAM Failure Type
NVSVBF	VBFNRF	Number of BIND Failures
NVSVBF	VBFRCODE	UNBIND/BIND Failure Code

2.3.4.1.2 Reliability Exceptions

The standard exceptions listed below may be applicable when analyzing network reliability. These exceptions indicate that installation-defined error thresholds have been exceeded. The exception reporting provided with the CA MICS Network Analyzer is discussed in Chapter 4. Detailed descriptions are provided for each of the exceptions.

- o 12002 - Link Error Count Threshold Exceeded
- o 12061 - Network Component Error Threshold Exceeded
- o 12183 - Network Component Error Rate Exceeds Limit
- o 12193 - Percentage of Bytes Retransmitted Exceeds Limit
- o 12541 - NPDA Event
- o 12542 - NPDA Event Alert
- o 12601 - NPDA Statistical Alert
- o 12852 - Invalid Session Parameters Threshold Exceeded
- o 12853 - Virtual Route Inoperative Threshold Exceeded
- o 12854 - Route Extension Inoperative Threshold Exceeded
- o 12855 - Hierarchical Reset Threshold Exceeded
- o 12856 - SSCP Gone Threshold Exceeded
- o 12857 - Virtual Route Deactivated Threshold Exceeded
- o 12858 - LU Failure - Unrecoverable Threshold Exceeded
- o 12859 - LU Failure - Recoverable Threshold Exceeded
- o 12862 - Session Failure Threshold Exceeded

2.3.4.1.3 Reliability Reports

The standard reports listed below may be applicable when analyzing network reliability. These reports are described in Chapter 3.

TABULAR REPORTS

- o SNT209 - NPM/NetSpy NCP Workload by Link Report
- o SNT215 - NPM/NetSpy NCP Workload by Link Report
- o SNT216 - NPM/NetSpy NCP Workload by Link Report
- o SNT401 - NPM NCP Data Collection Report
- o SNT401 - CA NetSpy NCP Data Collection Report
- o SNT601 - NPDA Event Analysis Report
- o SNT602 - NPDA Statistics Analysis Report

GRAPHIC INQUIRIES

- o SNTG301 - Error Count for Link
- o SNTG302 - Percent Temporary Errors to Traffic
- o SNTG303 - NPDA Events for Cluster Controller

MICF INQUIRIES

- o SNTCD9 NPM Daily Link Error Count
- o SNTCDA NetView Daily % Link Errors to Traffic
- o SNTCDB NetView Daily NPDA Events Summary
- o SNTCWJ NetView Weekly Abnormal UNBINDs by PLU
- o SNTPD9 NPM/NetSpy Daily Link Error Count By Hour
- o SNTPW0 NetView Weekly Abnormal UNBIND Report

Note that any report listed above that begins with the name of the data source NetView NLDM can also be produced from equivalent data collected by CA NetMaster NTS. Any report beginning with the name of the data source NetView NPDA can also be produced from equivalent data collected by CA NetMaster NEWS.

2.3.4.1.4 Reliability Analysis

Mean-Time-Between-Failures (MTBF) is one of the most widely used measures of device reliability. MTBF figures are used to schedule routine maintenance, determine the requirements for backup equipment, compare the reliability of a given device to industry or installation standards, or aid in the selection of competing equipment models.

Tracking the rate of change of MTBF statistics over time can also yield valuable results. Decreasing MTBF values can foreshadow the end of the practical useful life of a device. Conversely, increasing MTBF values are sometimes encountered in installations which utilize heavily microcoded, "intelligent" devices such as point-of-sale or financial controllers. These devices may experience random hard failures due to undiscovered microcode errors. A significant increase in MTBF following a microcode update may indicate that such a "bug" was fixed.

MTBF statistics are easily reported using the data retained by CA MICS in the NPDA Event (SNTNEF) File. Each entry in this file in the DETAIL time-span records the occurrence of a permanent error on a specific device. In the higher timespans (DAYS, WEEKS, MONTHS, and YEARS), the number of failures of a given type are summarized for each device in the variable Number of Events (NEFNREVT). Since basic MTBF statistics are based on the total number of failures, the data must be summarized across all types of failures. This can easily be done using the CA MICS Summarization Facility as follows:

```
%INCLUDE INCLLIB(#SNTSUM);
MACRO _BY NEFFRNAM %
MACRO _BREAK NEFFRNAM %
PROC SORT DATA=_dSNTM.SNTNEF01 OUT=MTBF; BY _BY;
RUN;

DATA MTBF; SET MTBF; BY _BY;
      _NEFSUM
RUN;

DATA MTBF (KEEP=NEFFRNAM MTBF);
FORMAT MTBF TIME.;
LABEL MTBF=MEAN-TIME-BETWEEN-FAILURES;
MTBF = (ENDTS-STARTTS) / NEFNREVT;
RUN;

PROC PRINT LABEL;
```

```
VAR NEFFRNAM MTBF;  
TITLE1 'MEAN-TIME-BETWEEN-FAILURE STATISTICS';  
RUN;
```

2.3.4.2 Environment: Capacity Management

Capacity management in the data communications environment can be approached in two ways:

- o Workload Growth Analysis
- o Service Degradation Analysis

Workload growth analysis is an extension of the traditional utilization-centered, capacity management strategy which has been successfully employed in the mainframe environment. Workload growth analysis is particularly effective in the early life of a given network configuration where load balancing may be a key performance improvement strategy.

Service degradation analysis interprets network capacity in terms of the ability to deliver network services in a timely manner. In some cases, service levels vary in inverse proportion to network load. In these cases, poor service may limit network utilization ("...response is so bad we don't use it...") well below the threshold of utilization overload as indicated by a workload growth study.

The trend format of both the workload and utilization reports provided with the CA MICS Network Analyzer are designed to help you implement either of these strategies.

One area of particular concern is the group of communications control units (and their associated NCPs) which make up the network backbone. Over-utilization and its associated service degradation tend to occur first in the backbone because the traffic is concentrated there. Close attention should be paid to the percentage utilization and time in slowdown on these CCUs.

The following sections suggest key data elements, exception conditions, reports, and sample analysis which may be helpful in network capacity management:

- 1 - Capacity Management Indicators
- 2 - Capacity Management Exceptions
- 3 - Capacity Management Reports
- 4 - Capacity Analysis

2.3.4.2.1 Capacity Management Indicators

In preparing reports for dissemination to Information Systems and user management, it is important that the measures reported are understandable and pertinent to the subject being reported. The data elements listed below best represent the data elements you may use to report network service levels. These elements are discussed in detail in Appendix B, which contains the Network (SNT) and the NetView Session (NVS) Information Areas.

```
-----  
|  MANAGEMENT AREA:  Environment  |  
|    ACTIVITY AREA:  Capacity    |  
|    RESPONSIBILITY AREA:  Network  |  
-----
```

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNCL	NCLNRRLS	Receiving Link Speed
SNTNCL	NCLNRSLS	Sending Link Speed
SNTNCL	NCLNRCHR	Number of Bytes Received
SNTNCL	NCLNRCHS	Number of Bytes Sent
SNTNCL	NCLNRIFR	Number of I-Frames Received
SNTNCL	NCLNRIFS	Number of I-Frames Sent
SNTNCL	NCLNRMSR	Number of Messages Received
SNTNCL	NCLNRMSS	Number of Messages Sent
SNTNCL	NCLNRERR	Error Count
SNTNCL	NCLNRRBY	Retransmit Byte Count
SNTNCL	NCLNRRIF	Retransmit I-Frame Count
SNTNCL	NCLNRROQ	Resource Outbound Queue Length
SNTNCL	NCLNRRRR	Total RNR Frames Received
SNTNCL	NCLNRRRS	Total RNR Frames Sent
SNTNCL	NCLNRRFR	Total RR Frames Received
SNTNCL	NCLNRRFS	Total RR Frames Sent
SNTNCL	NCLNRRFD	Number of Receive Frames Discarded
SNTNCL	NCLNRRFM	Number of Receive Frames Misaddressed
SNTNCL	NCLNRRFU	Number of Receive Frames Unrecognized
SNTNCL	NCLMXROQ	Max. Resource Outbound Queue Length
SNTNCL	NCLPCELBS	Percent Link Busy Retransmission
SNTNCL	NCLPCLBS	Percent Link Busy
SNTNCL	NCLMXLBS	Max. Percent Link Busy
SNTNCL	NCLMNLBS	Min. Percent Link Busy
SNTNCL	NCLPCRLB	Percent Link Busy Receiving
SNTNCL	NCLMXRLB	Max. Percent Link Busy Receiving
SNTNCL	NCLMNLB	Min. Percent Link Busy Receiving
SNTNCL	NCLPCSLB	Percent Link Busy Sending
SNTNCL	NCLMXSLB	Max. Percent Link Busy Sending
SNTNCL	NCLMNSLB	Min. Percent Link Busy Sending

SNTNCL	NCLPMCHR	Number of Bytes Received per Minute
SNTNCL	NCLPMCHS	Number of Bytes Sent per Minute
SNTNCL	NCLPMIFR	Number of I-Frames Received per Minute
SNTNCL	NCLPMIFS	Number of I-Frames Sent per Minute
SNTNCL	NCLPMMSR	Number of Messages Received per Minute
SNTNCL	NCLPMMS	Number of Messages Sent per Minute
SNTNCL	NCLPMTPL	Number of Total Polls per Minute

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTCAF	CAFNRRLS	Receiving Link Speed
SNTCAF	CAFNRSLs	Sending Link Speed
SNTCAF	CAFNRCHR	Number of Bytes Received
SNTCAF	CAFNRCHS	Number of Bytes Sent
SNTCAF	CAFNRMSR	Number of Messages Received
SNTCAF	CAFNRMS	Number of Messages Sent
SNTCAF	CAFNRPKR	Number of Packets Received
SNTCAF	CAFNRPKS	Number of Packets Sent
SNTCAF	CAFNRERR	Error Count
SNTCAF	CAFNRBY	Retransmit Byte Count
SNTCAF	CAFNRROQ	Resource Outbound Queue Length
SNTCAF	CAFNRIFS	Number of I-Frames Sent
SNTCAF	CAFNRIFR	Number of I-Frames Received
SNTCAF	CAFNRRIIF	Retransmitted I-Frame Count
SNTCAF	CAFNRFRS	Number of Frames Sent
SNTCAF	CAFNRFRR	Number of Frames Received
SNTCAF	CAFNRRT0	Reply Timeouts
SNTCAF	CAFNRLB0	Local Busy Occurrences
SNTCAF	CAFNRSFS	Rejected Supervisor Frames Sent
SNTCAF	CAFNRSFR	Rejected Supervisor Frames Received
SNTCAF	CAFMRXROQ	Max. Resource Outbound Queue Length
SNTCAF	CAFPMCHR	Number of Bytes Received per Minute
SNTCAF	CAFPMCHS	Number of Bytes Sent per Minute
SNTCAF	CAFPMMSR	Number of Messages Received per Minute
SNTCAF	CAFPMMS	Number of Messages Sent per Minute
SNTCAF	CAFPMMPKR	Number of Packets Received per Minute
SNTCAF	CAFPMMPKS	Number of Packets Sent per Minute
SNTCAF	CAFPMTPL	Number of Total Polls per Minute
SNTCAF	CAFIDITM	Idle Interval Time

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNAF	NAFMNFB	Free Buffer Low Water Mark
SNTNAF	NAFMNFBQ	Minimum Free Buffer Queue Length
SNTNAF	NAFMNHQL	Minimum Channel Hold Queue Length
SNTNAF	NAFMNIQL	Minimum Channel Intermed. Queue Length
SNTNAF	NAFMNSFB	Minimum Free Buffer Count at Slowdown
SNTNAF	NAFMXANP	Max Available NCP Buffers
SNTNAF	NAFMXFBH	Free Buffer High Water Mark

SNTNAF	NAFMXFBQ	Maximum Free Buffer Queue Length
SNTNAF	NAFMXHQL	Maximum Channel Hold Queue Length
SNTNAF	NAFMXIQL	Maximum Channel Intermed. Queue Length
SNTNAF	NAFMXSFB	Maximum Free Buffer Count at Slowdown
SNTNAF	NAFAVFBQ	Average Free Buffer Queue Length
SNTNAF	NAFAVHQL	Average NCP Channel Hold Queue Length
SNTNAF	NAFAVIQL	Average NCP Channel Intermed. Queue Len.
SNTNAF	NAFAVSFB	Average Free Buffer Count at Slowdown
SNTNAF	NAFPCCCU	Percent Communications Controller Util.
SNTNAF	NAFMXCCU	Maximum Percent CCU Utilization
SNTNAF	NAFMNCCU	Minimum Percent CCU Utilization
SNTNAF	NAFPCNBU	Percent NCP Buffer Util.
SNTNAF	NAFMXNBU	Max. Percent NCP Buffer Util.
SNTNAF	NAFMNNBU	Min. Percent NCP Buffer Util.
SNTNAF	NAFPCTIS	Percent Time in Slowdown

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTPSU	PSUBRESC	Response Event Count (Both)
SNTPSU	PSUNRFMR	Number Text Bytes Received
SNTPSU	PSUNRFMS	Number Text Bytes Sent
SNTPSU	PSUNRNFR	Number Control Bytes Received
SNTPSU	PSUNRMFS	Number Control Bytes Sent
SNTPSU	PSUNRPFR	Number Text PIUs Received
SNTPSU	PSUNRPFS	Number Text PIUs Sent
SNTPSU	PSUNRPNR	Number Control PIUs Received
SNTPSU	PSUNRPNS	Number Control PIUs Sent
SNTPSU	PSUNRMBR	No. of Text Message Bytes Rec'd
SNTPSU	PSUNRMBS	No. of Text Message Bytes Sent
SNTPSU	PSUNRMSR	Number of Text Messages Rec'd
SNTPSU	PSUNRMSS	Number of Text Messages Sent
SNTPSU	PSUMXMBR	Max Text Message Rec'd
SNTPSU	PSUMXMBS	Max Text Message Sent
SNTPSU	PSUMXTBR	Max Text PIU Rec'd
SNTPSU	PSUMXTBS	Max Text PIU Sent
SNTPSU	PSUAVNTM	Average Network Response Time
SNTPSU	PSUAVHTM	Average Host Response Time
SNTPSU	PSUAVTTM	Average Total Response Time
SNTPSU	PSUBRESC	Response Event Count (Both)
SNTPSU	PSUPCBR1	Cum. Pct Both Resp Within Limit 1
SNTPSU	PSUPCBR2	Cum. Pct Both Resp Within Limit 2
SNTPSU	PSUPCBR3	Cum. Pct Both Resp Within Limit 3
SNTPSU	PSUPCBR4	Cum. Pct Both Resp Within Limit 4
SNTPSU	PSUPCHR1	Cum. Pct Host Resp Within Limit 1
SNTPSU	PSUPCHR2	Cum. Pct Host Resp Within Limit 2
SNTPSU	PSUPCHR3	Cum. Pct Host Resp Within Limit 3
SNTPSU	PSUPCHR4	Cum. Pct Host Resp Within Limit 4
SNTPSU	PSUPCTR1	Cum. Pct Total Resp Within Limit 1
SNTPSU	PSUPCTR2	Cum. Pct Total Resp Within Limit 2

SNTPSU	PSUPCTR3	Cum. Pct Total Resp Within Limit 3
SNTPSU	PSUPCNON	Pct of Total Events W/out Netwk Resp
SNTPSU	PSUTDST1	Response Distribution Count 1 (Total)
SNTPSU	PSUTDST2	Response Distribution Count 2 (Total)
SNTPSU	PSUTDST3	Response Distribution Count 3 (Total)
SNTPSU	PSUTDST4	Response Distribution Count 4 (Total)
SNTPSU	PSUTDST5	Response Distribution Count 5 (Total)
SNTPSU	PSUMXHTM	Maximum Host Resp Time
SNTPSU	PSUMXNTM	Maximum Net Resp Time (w/ Host Tx)
SNTPSU	PSUMXTTM	Maximum Total Resp Time
SNTPSU	PSUERQTM	Total Time Exceeded Squared
SNTPSU	PSUERTTM	Total Time Oper Threshold Exceeded
SNTPSU	PSUHRQTM	Host Response Time Squared
SNTPSU	PSUNNHTM	Net Resp Time
SNTPSU	PSUNRHO	Number of Host Only Transactions
SNTPSU	PSUNRNNH	Resp Event Count (Net)
SNTPSU	PSUNRQTM	Net Response Time Squared (w/ Host Tx)
SNTPSU	PSUORQTM	Net Response Time Squared
SNTPSU	PSUTRQTM	Total Resp Time Squared
SNTPSU	PSUMXNNH	Maximum Network Resp Time

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTPSY	PSYBRES	Response Event Count (Both)
SNTPSY	PSYNRFMR	Number Text Bytes Received
SNTPSY	PSYNRFMS	Number Text Bytes Sent
SNTPSY	PSYNRNFR	Number Control Bytes Received
SNTPSY	PSYNRMFS	Number Control Bytes Sent
SNTPSY	PSYNRPFR	Number Text PIUs Received
SNTPSY	PSYNRPFS	Number Text PIUs Sent
SNTPSY	PSYNRPNR	Number Control PIUs Received
SNTPSY	PSYNRPNS	Number Control PIUs Sent
SNTPSY	PSYNRHO	Number of Host Only Transactions
SNTPSY	PSYNRMBR	No. of Text Message Bytes Rec'd
SNTPSY	PSYNRMBS	No. of Text Message Bytes Sent
SNTPSY	PSYNRMSR	No. of Text Messages Rec'd
SNTPSY	PSYNRMSS	No. of Text Messages Sent
SNTPSY	PSYMXMBR	Max Text Message Rec'd
SNTPSY	PSYMXMBS	Max Text Message Sent
SNTPSY	PSYMXTBR	Max Text PIU Rec'd
SNTPSY	PSYMXTBS	Max Text PIU Sent
SNTPSY	PSYAVNTM	Average Network Response Time
SNTPSY	PSYAVHTM	Average Host Response Time
SNTPSY	PSYAVTTM	Average Total Response Time
SNTPSY	PSYBRES	Response Event Count (Both)
SNTPSY	PSYPCBR1	Cum. Pct Both Resp Within Limit 1
SNTPSY	PSYPCBR2	Cum. Pct Both Resp Within Limit 2
SNTPSY	PSYPCBR3	Cum. Pct Both Resp Within Limit 3
SNTPSY	PSYPCBR4	Cum. Pct Both Resp Within Limit 4

SNTPSY	PSYPCHR1	Cum. Pct Host Resp Within Limit 1
SNTPSY	PSYPCHR2	Cum. Pct Host Resp Within Limit 2
SNTPSY	PSYPCHR3	Cum. Pct Host Resp Within Limit 3
SNTPSY	PSYPCHR4	Cum. Pct Host Resp Within Limit 4
SNTPSY	PSYPCTR1	Cum. Pct Total Resp Within Limit 1
SNTPSY	PSYPCTR2	Cum. Pct Total Resp Within Limit 2
SNTPSY	PSYPCTR3	Cum. Pct Total Resp Within Limit 3
SNTPSY	PSYPCNON	Pct of Total Events W/out Netwk Resp
SNTPSY	PSYTDST1	Response Distribution Count 1 (Total)
SNTPSY	PSYTDST2	Response Distribution Count 2 (Total)
SNTPSY	PSYTDST3	Response Distribution Count 3 (Total)
SNTPSY	PSYTDST4	Response Distribution Count 4 (Total)
SNTPSY	PSYTDST5	Response Distribution Count 5 (Total)
SNTPSY	PSYMXHTM	Maximum Host Resp Time
SNTPSY	PSYMXNTM	Maximum Net Resp Time (w/ Host Tx)
SNTPSY	PSYMXTTM	Maximum Total Resp Time
SNTPSY	PSYERQTM	Total Time Exceeded Squared
SNTPSY	PSYERTTM	Total Time Oper Threshold Exceeded
SNTPSY	PSYHRQTM	Host Response Time Squared
SNTPSY	PSYNNHTM	Net Resp Time
SNTPSY	PSYNRHO	No. of Host Only Transactions
SNTPSY	PSYNNNH	Resp Event Count (Net)
SNTPSY	PSYNRQTM	Net Resp Time Squared (w/ Host Tx)
SNTPSY	PSYORQTM	Net Resp Time Squared
SNTPSY	PSYTRQTM	Total Resp Time Squared
SNTPSY	PSYMXNNH	Maximum Network Resp Time

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNPL	NPLBRES	Response Event Count (Both)
SNTNPL	NPLNRFMR	Number Text Bytes Received
SNTNPL	NPLNRFMS	Number Text Bytes Sent
SNTNPL	NPLNRNFR	Number Control Bytes Received
SNTNPL	NPLNRMFS	Number Control Bytes Sent
SNTNPL	NPLNRPFR	Number Text PIUs Received
SNTNPL	NPLNRPFS	Number Text PIUs Sent
SNTNPL	NPLNRPNR	Number Control PIUs Received
SNTNPL	NPLNRPNS	Number Control PIUs Sent
SNTNPL	NPLNRMBR	No. of Text Message Bytes Rec'd
SNTNPL	NPLNRMBS	No. of Text Message Bytes Sent
SNTNPL	NPLNRMSR	No. of Text Messages Rec'd
SNTNPL	NPLNRMSS	No. of Text Messages Sent
SNTNPL	NPLMXMBR	Max Text Message Rec'd
SNTNPL	NPLMXMBS	Max Text Message Sent
SNTNPL	NPLMXTBR	Max Text PIU Rec'd
SNTNPL	NPLMXTBS	Max Text PIU Sent
SNTNPL	NPLAVNTM	Average Network Response Time
SNTNPL	NPLAVHTM	Average Host Response Time
SNTNPL	NPLAVTTM	Average Total Response Time

SNTNPL	NPLBRES	Response Event Count (Both)
SNTNPL	NPLPCBR1	Cum. Pct Both Resp Within Limit 1
SNTNPL	NPLPCBR2	Cum. Pct Both Resp Within Limit 2
SNTNPL	NPLPCBR3	Cum. Pct Both Resp Within Limit 3
SNTNPL	NPLPCBR4	Cum. Pct Both Resp Within Limit 4
SNTNPL	NPLPCHR1	Cum. Pct Host Resp Within Limit 1
SNTNPL	NPLPCHR2	Cum. Pct Host Resp Within Limit 2
SNTNPL	NPLPCHR3	Cum. Pct Host Resp Within Limit 3
SNTNPL	NPLPCHR4	Cum. Pct Host Resp Within Limit 4
SNTNPL	NPLPCTR1	Cum. Pct Total Resp Within Limit 1
SNTNPL	NPLPCTR2	Cum. Pct Total Resp Within Limit 2
SNTNPL	NPLPCTR3	Cum. Pct Total Resp Within Limit 3
SNTNPL	NPLPCNON	Pct of Total Events W/out Netwk Resp
SNTNPL	NPLTDST1	Response Distribution Count 1 (Total)
SNTNPL	NPLTDST2	Response Distribution Count 2 (Total)
SNTNPL	NPLTDST3	Response Distribution Count 3 (Total)
SNTNPL	NPLTDST4	Response Distribution Count 4 (Total)
SNTNPL	NPLTDST5	Response Distribution Count 5 (Total)
SNTNPL	NPLMXHTM	Maximum Host Resp Time
SNTNPL	NPLMXNTM	Maximum Net Resp Time (w/ Host Tx)
SNTNPL	NPLMXTTM	Maximum Total Resp Time
SNTNPL	NPLERQTM	Total Time Exceeded Squared
SNTNPL	NPLERTTM	Total Time Oper Threshold Exceeded
SNTNPL	NPLHRQTM	Host Response Time Squared
SNTNPL	NPLNNHTM	Net Resp Time
SNTNPL	NPLNRHO	Number of Host Only Transactions
SNTNPL	NPLNRNNH	Resp Event Count (Net)
SNTNPL	NPLNRQTM	Net Response Time Squared (w/ Host Tx)
SNTNPL	NPLORQTM	Net Resp Time Squared
SNTNPL	NPLTRQTM	Total Resp Time Squared
SNTNPL	NPLMXNNH	Maximum Network Resp Time

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNSV	NSVCOS	Class of Service
SNTNSV	NSVPCOBJ	Objective Percentage
SNTNSV	NSVROBTM	Objective Response Time
SNTNSV	NSVTRESC	Total Response Event Count
SNTNSV	NSVAVTM	Average Total Response TIme
SNTNSV	NSVPCOBM	Pct of Times Response Obj Met
SNTNSV	NSVPCTR1	Cum. Pct All Response Within Limit 1
SNTNSV	NSVPCTR2	Cum. Pct All Response Within Limit 2
SNTNSV	NSVPCTR3	Cum. Pct All Response Within Limit 3
SNTNSV	NSVPCTR4	Cum. Pct All Response Within Limit 4

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
NVSLSY	LSYCOS	Class of Service
NVSLSY	LSYNRCBR	Number Control Bytes Received

NVSLSY	LSYNRCBS	Number Control Bytes Sent
NVSLSY	LSYNRCPR	Number Control PIUs Received
NVSLSY	LSYNRCPS	Number Control PIUs Sent
NVSLSY	LSYNRTBR	Number Text Bytes Received
NVSLSY	LSYNRTBS	Number Text Bytes Sent
NVSLSY	LSYNRTPR	Number Text PIUs Received
NVSLSY	LSYNRTPS	Number Text PIUs Sent
NVSLSY	LSYPCOBJ	Objective Percentage
NVSLSY	LSYPCOBM	Pct of Times Response Obj Met
NVSLSY	LSYPCTR1	Cum. Pct All Resp Within Limit 1
NVSLSY	LSYPCTR2	Cum. Pct All Resp Within Limit 2
NVSLSY	LSYPCTR3	Cum. Pct All Resp Within Limit 3
NVSLSY	LSYPCTR4	Cum. Pct All Resp Within Limit 4
NVSLSY	LSYROBTM	Objective Response Time
NVSLSY	LSYTRESC	Response Event Count

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
NVSNLL	NLLCOS	Class of Service
NVSNLL	NLLNRCBR	Number Control Bytes Received
NVSNLL	NLLNRCBS	Number Control Bytes Sent
NVSNLL	NLLNRCPR	Number Control PIUs Received
NVSNLL	NLLNRCPS	Number Control PIUs Sent
NVSNLL	NLLNRTBR	Number Text Bytes Received
NVSNLL	NLLNRTBS	Number Text Bytes Sent
NVSNLL	NLLNRTPR	Number Text PIUs Received
NVSNLL	NLLNRTPS	Number Text PIUs Sent
NVSNLL	NLLPCOBJ	Objective Percentage
NVSNLL	NLLPCOBM	Pct of Times Response Obj Met
NVSNLL	NLLPCTR1	Cum. Pct All Resp Within Limit 1
NVSNLL	NLLPCTR2	Cum. Pct All Resp Within Limit 2
NVSNLL	NLLPCTR3	Cum. Pct All Resp Within Limit 3
NVSNLL	NLLPCTR4	Cum. Pct All Resp Within Limit 4
NVSNLL	NLLROBTM	Objective Response Time

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
NVNSA	NSACONTM	Connect Time
NVNSA	NSANRCBR	Number Control Bytes Received
NVNSA	NSANRCBS	Number Control Bytes Sent
NVNSA	NSANRCPR	Number Control PIUs Received
NVNSA	NSANRCPS	Number Control PIUs Sent
NVNSA	NSANRTBR	Number Text Bytes Received
NVNSA	NSANRTBS	Number Text Bytes Sent
NVNSA	NSANRTBY	Total Number of Bytes Transmitted
NVNSA	NSANRTPI	Total Number of PIUs Transmitted
NVNSA	NSANRTPR	Number Text PIUs Received
NVNSA	NSANRTPS	Number Text PIUs Sent

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
NVNSNC	NSCCONTM	Connect Time
NVNSNC	NSCNMSES	Number of Sessions
NVNSNC	NSCNRTCH	Total Characters Transmitted
FILE	ELEMENT	DESCRIPTION
-----	-----	-----
NVSRTE	RTECONTM	Connect Time
NVSRTE	RTENRTCH	Total Characters Transmitted
FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNSP	NSPNRBYR	Cumulative Bytes Received
SNTNSP	NSPNRBYS	Cumulative Bytes Sent
SNTNSP	NSPNRESC	Network Responses
SNTNSP	NSPNROUT	Number of Outputs
SNTNSP	NSPNRTRI	Number of Transactions (LU62 Sessions)
SNTNSP	NSPTRESC	Number of Transactions (# of Inputs)
FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNSS	NSSNRBYR	Cumulative Bytes Received
SNTNSS	NSSNRBYS	Cumulative Bytes Sent
SNTNSS	NSSNRBYT	Cumulative Bytes Transmitted
SNTNSS	NSSNRESC	Network Responses
SNTNSS	NSSNROUT	Number of Outputs
SNTNSS	NSSNRTRI	Number of Transactions (LU62 Sessions)
SNTNSS	NSSTRESC	Number of Transactions (# of Inputs)
FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNVR	NVRNRBYS	Cumulative Bytes Sent
SNTNVR	NVRNRMOP	Measured Outbound PIUs
SNTNVR	NVRNRTOP	Total Outbound PIUs
SNTNVR	NVRAVPL	Average Outbound PIU Length
SNTNVR	NVRNRESC	Network Responses (Measured)
FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNAC	NACCONTM	Connect Time
SNTNAC	NACNRCBR	Number Control Bytes Received
SNTNAC	NACNRCBS	Number Control Bytes Sent
SNTNAC	NACNRCPR	Number Control PIUs Received
SNTNAC	NACNRCPS	Number Control PIUs Sent
SNTNAC	NACNRTBR	Number Text Bytes Received
SNTNAC	NACNRTBS	Number Text Bytes Sent
SNTNAC	NACNRTBY	Total Number of Bytes Transmitted
SNTNAC	NACNRTPI	Total Number of PIUs Transmitted

SNTNAC	NACNRTPR	Number	Text	PIUs Received
SNTNAC	NACNRTPS	Number	Text	PIUs Sent

2.3.4.2.2 Capacity Management Exceptions

The standard exceptions listed below may have applicability when analyzing network capacity. These exceptions pinpoint events that can indicate insufficient capacity in one or more network resources. The exception reporting provided with this product is discussed in Chapter 4. Detailed descriptions are provided for each of the exceptions.

- o 12001 - Link Average Utilization Threshold Exceeded
- o 12003 - Link Resource Outbound Queue Length Exceeded
- o 12004 - Link Polling Rate Below Threshold
- o 12005 - Link Positive Polling Percentage Threshold Exceeded
- o 12062 - Component Resource Outbound Q Length Exceeded
- o 12121 - 37XX Utilization Threshold Exceed
- o 12122 - Percentage CCU Time in Slowdown Threshold Exceeded
- o 12123 - Average Free Buffer Queue Length Below Limit
- o 12124 - Avg NCP Channel Hold Q Length Threshold Exceeded
- o 12181 - Network Component Traffic Exceeds Limit
- o 12182 - Network Component Traffic Below Minimum
- o 12184 - NCP Processor Overloaded
- o 12185 - NCP Processor Under-utilized
- o 12186 - Negative Poll Rate Exceeds Limit
- o 12187 - Positive Poll Rate Below Limit
- o 12188 - Messages Per Minute Exceeds Limit
- o 12189 - Bytes Per Second Exceeds Limit
- o 12190 - Percentage of Free Buffers Below Minimum
- o 12191 - Outbound Queue Length Exceeds Limit
- o 12192 - Percentage of Time in Slowdown Exceeds Limit
- o 12194 - Percentage of NCP Buffers Used Exceeds Limit
- o 12301 - Response Objective Missed For Performance Class
- o 12541 - NPDA Event
- o 12542 - NPDA Event Alert
- o 12601 - NPDA Statistical Alert
- o 12661 - Host Response Outside Bounds-Count Exceeded for SLU
- o 12662 - Net Response Outside Bounds-Count Exceeded for SLU
- o 12663 - Total Response Outside Bounds-Count Exceeded for SLU
- o 12780 - Host Response Outside Bounds-Count Exceeded for Link
- o 12781 - Net Response Outside Bounds-Count Exceeded for Link
- o 12782 - Total Response Outside Bounds-Count Exceeded

for Link

2.3.4.2.3 Capacity Management Reports

The standard reports listed below are useful for analyzing network capacity. These reports are described in Chapter 3.

TABULAR REPORTS

- o SNT101 - NPM Service by Application Report
- o SNT103 - NPM Service by Link Report
- o SNT121 - CA NetSpy Service by Application
- o SNT122 - CA NetSpy Service by Terminal
- o SNT201 - NPM Workload by Application Report
- o SNT203 - NPM Workload by Link Report
- o SNT208 - NPM/NetSpy Utilization by NCP Report
- o SNT209 - NPM/NetSpy NCP Workload by Link Report
- o SNT211 - NLDM Workload by Application
- o SNT212 - NLDM Workload by Link
- o SNT213 - NLDM Workload by Control Unit
- o SNT214 - NLDM Workload by Terminal
- o SNT215 - NPM/NetSpy NCP Workload by Link Report
- o SNT216 - NPM/NetSpy NCP Workload by Link Report
- o SNT221 - CA NetSpy Workload by Application
- o SNT222 - CA NetSpy Workload by Terminal
- o SNT401 - NPM NCP Data Collection Report
- o SNT401 - CA NetSpy NCP Data Collection Report
- o SNT403 - NPM Session Data Collection Report

GRAPHIC INQUIRIES

- o SNTG101 - Average Response by Performance Class
- o SNTG102 - Application Service Analysis
- o SNTG103 - Application Service Analysis by Hour
- o SNTG201 - Traffic Profile Report for Link
- o SNTG202 - Communications Controller Utilization Profile
- o SNTG203 - NCP Buffer Utilization Trend
- o SNTG204 - Percent Link Utilization by Zone

MICF INQUIRIES

- o SNTCD6 NPM Daily Pct. NCP Cycle Util.
- o SNTCD7 NPM Daily NCP Buffer Utilization
- o SNTCD8 NPM Daily Link Utilization
- o SNTCDP CA NetSpy Daily Pct. NCP Cycle Util.
- o SNTCDQ CA NetSpy Daily NCP Buffer Utilization
- o SNTCDR CA NetSpy Daily Link Utilization
- o SNTCDC NetView Daily Connect Time by SNTACT1

- o SNTCDD NetView Daily Chars/1000 by SNTACT1
- o SNTCDE NetView Daily Chars/1000 by VR
- o SNTCDF NetView Daily Data Chars/1000 by SNTACT1
- o SNTCDG NetView Daily Cntl Chars/1000 by SNTACT1
- o SNTCWH NetView Weekly Cntl PIU Traffic by PLU
- o SNTCWK NetView Weekly Data PIU Traffic by PLU
- o SNTCDX NSA/NGA Daily Data Chars/1000 by SNTACT1
- o SNTCDY NSA/NGA Daily Data PIU Traffic by SNTACT1

Note that any report listed above that begins with the name of the data source NetView NLDM can also be produced from equivalent data collected by CA NetMaster NTS. Any report beginning with the name of the data source NetView NPDA can also be produced from equivalent data collected by CA NetMaster NEWS.

2.3.4.2.4 Capacity Analysis

Capacity management is the process of apportioning limited resources among different workloads based on the time allotted to process each workload. In most systems, the instantaneous arrival rate of work exceeds the instantaneous processing capacity at certain times, thus some work must wait while other work is performed.

The longer the acceptable window of processing (response time, in communication terms) for each transaction relative to the actual time required to process, the fewer processing resources are required to support the workload. Conversely, the shorter the processing window, the greater the resource requirement. In other words, workloads with infinitely long processing times can be satisfied by systems with very small processing capabilities per unit time (on a mainframe these are background tasks). However, workloads with infinitely short processing times require an infinite amount of resources to satisfy (these are all the applications for which you are responsible).

In a network, available resources include:

- o Processor power -- both mainframe and communications control units
- o Storage -- both mainframe and CCU memory and mainframe peripheral storage (databases)
- o Link bandwidth -- most critical in the network backbone

It is the interrelationship of these resources that makes the projection of network capacity difficult. Some of these interrelations are the following:

- o Insufficient processor power increases queuing, thus increasing the demand for storage and reducing the ability to utilize link bandwidth.
- o Insufficient storage in one node increases its processor requirements and increases queuing in adjacent nodes, increasing their storage requirements. It also reduces the ability of all nodes to support increased link bandwidth.
- o Insufficient link bandwidth increases storage requirements through increased queuing.

The network analyst must remember that a change to any node or link, either in capacity or workload, affects all adjacent nodes and the links attached to them.

2.3.4.3 Environment: Performance Management

Performance management is difficult to distinguish as a discrete activity within the scope of network management. In general, the majority of work in the network area can be categorized as either looking for areas where problems exist or looking for ways to solve them. These tasks are, of course, at the heart of performance management.

Within the network, performance is defined in terms of the service levels provided to the end-user. Therefore, it is mandatory that an installation define comprehensive service objectives as a basis for the performance management effort.

Once the objectives have been defined, the network performance group should track the actual service relative to the objectives on a daily basis. Service must be measured over small increments of time to prevent averaging from obscuring the peaks which constitute the problems.

The following sections suggest key data elements, exception conditions, component reports, and sample analyses which may be helpful in network performance management:

- 1 - Performance Management Indicators
- 2 - Performance Management Exceptions
- 3 - Performance Management Reports
- 4 - Performance Analysis

2.3.4.3.1 Performance Management Indicators

In preparing reports for dissemination, it is important that the measures reported are understandable and relevant to the subject being reported. The data elements listed below best represent the data elements you may use to report network service levels. These elements are discussed in detail in Appendix B, which contains the Network (SNT) and NetView Session (NVS) Information Areas.

```

-----
|  MANAGEMENT AREA:  Environment          |
|    ACTIVITY AREA:   Performance          |
|    RESPONSIBILITY AREA: Network          |
-----

```

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNCL	NCLNRRLS	Receiving Link Speed
SNTNCL	NCLNRSLS	Sending Link Speed
SNTNCL	NCLNRCHR	Number of Bytes Received
SNTNCL	NCLNRCHS	Number of Bytes Sent
SNTNCL	NCLNRIFR	Number of I-Frames Received
SNTNCL	NCLNRIFS	Number of I-Frames Sent
SNTNCL	NCLNRMSR	Number of Messages Received
SNTNCL	NCLNRMSS	Number of Messages Sent
SNTNCL	NCLNRERR	Error Count
SNTNCL	NCLNRRBY	Retransmit Byte Count
SNTNCL	NCLNRRIF	Retransmit I-Frame Count
SNTNCL	NCLNRRQ	Resource Outbound Queue Length
SNTNCL	NCLNRRRR	Total RNR Frames Received
SNTNCL	NCLNRRRS	Total RNR Frames Sent
SNTNCL	NCLNRRFR	Total RR Frames Received
SNTNCL	NCLNRRFS	Total RR Frames Sent
SNTNCL	NCLNRRFD	Number of Receive Frames Discarded
SNTNCL	NCLNRRFM	Number of Receive Frames Misaddressed
SNTNCL	NCLNRRFU	Number of Receive Frames Unrecognized
SNTNCL	NCLMXRQ	Max. Resource Outbound Queue Length
SNTNCL	NCLPCEL	Percent Link Busy Retransmission
SNTNCL	NCLPCLBS	Percent Link Busy
SNTNCL	NCLMXLBS	Max. Percent Link Busy
SNTNCL	NCLMNLBS	Min. Percent Link Busy
SNTNCL	NCLPCRLB	Percent Link Busy Receiving
SNTNCL	NCLMXRLB	Max. Percent Link Busy Receiving
SNTNCL	NCLMNLB	Min. Percent Link Busy Receiving
SNTNCL	NCLPCSLB	Percent Link Busy Sending
SNTNCL	NCLMXSLB	Max. Percent Link Busy Sending
SNTNCL	NCLMNSLB	Min. Percent Link Busy Sending

SNTNCL	NCLPMCHR	Number of Bytes Received per Minute
SNTNCL	NCLPMCHS	Number of Bytes Sent per Minute
SNTNCL	NCLPMIFR	Number of I-Frames Received per Minute
SNTNCL	NCLPMIFS	Number of I-Frames Sent per Minute
SNTNCL	NCLPMMSR	Number of Messages Received per Minute
SNTNCL	NCLPMMS	Number of Messages Sent per Minute
SNTNCL	NCLPMTPL	Number of Total Polls per Minute

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTCAF	CAFNRRLS	Receiving Link Speed
SNTCAF	CAFNRSLs	Sending Link Speed
SNTCAF	CAFNRCHR	Number of Bytes Received
SNTCAF	CAFNRCHS	Number of Bytes Sent
SNTCAF	CAFNRPKR	Number of Packets Received
SNTCAF	CAFNRPKS	Number of Packets Sent
SNTCAF	CAFNRMSR	Number of Messages Received
SNTCAF	CAFNRMS	Number of Messages Sent
SNTCAF	CAFNRERR	Error Count
SNTCAF	CAFNRBY	Retransmit Byte Count
SNTCAF	CAFNRROQ	Resource Outbound Queue Length
SNTCAF	CAFNRIFS	Number of I-Frames Sent
SNTCAF	CAFNRIFR	Number of I-Frames Received
SNTCAF	CAFNRRI	Retransmitted I-Frame Count
SNTCAF	CAFNRFRS	Number of Frames Sent
SNTCAF	CAFNRFR	Number of Frames Received
SNTCAF	CAFNRRT0	Reply Timeouts
SNTCAF	CAFNRLB0	Local Busy Occurrences
SNTCAF	CAFNRSFS	Rejected Supervisor Frames Sent
SNTCAF	CAFNRSFR	Rejected Supervisor Frames Received
SNTCAF	CAFMRXROQ	Max. Resource Outbound Queue Length
SNTCAF	CAFPMCHR	Number of Bytes Received per Minute
SNTCAF	CAFPMCHS	Number of Bytes Sent per Minute
SNTCAF	CAFMPMPKR	Number of Packets Received per Minute
SNTCAF	CAFMPMPKS	Number of Packets Sent per Minute
SNTCAF	CAFPMMSR	Number of Messages Received per Minute
SNTCAF	CAFPMMS	Number of Messages Sent per Minute
SNTCAF	CAFPMTPL	Number of Total Polls per Minute
SNTCAF	CAFIDITM	Idle Interval Time

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNAF	NAFMNFB	Free Buffer Low Water Mark
SNTNAF	NAFMNFBQ	Minimum Free Buffer Queue Length
SNTNAF	NAFMNHQL	Minimum Channel Hold Queue Length
SNTNAF	NAFMNIQL	Minimum Channel Intermed. Queue Length
SNTNAF	NAFMNSFB	Minimum Free Buffer Count at Slowdown
SNTNAF	NAFMXANP	Max Available NCP Buffers
SNTNAF	NAFMXFBH	Free Buffer High Water Mark

SNTNAF	NAFMXFBQ	Maximum Free Buffer Queue Length
SNTNAF	NAFMXHQL	Maximum Channel Hold Queue Length
SNTNAF	NAFMXIQL	Maximum Channel Intermed. Queue Length
SNTNAF	NAFMXSFB	Maximum Free Buffer Count at Slowdown
SNTNAF	NAFAVFBQ	Average Free Buffer Queue Length
SNTNAF	NAFAVHQL	Average NCP Channel Hold Queue Length
SNTNAF	NAFAVIQL	Average NCP Channel Intermed. Queue Len.
SNTNAF	NAFAVSFB	Average Free Buffer Count at Slowdown
SNTNAF	NAFPCCCU	Percent Communications Controller Util.
SNTNAF	NAFMXCCU	Maximum Percent CCU Utilization
SNTNAF	NAFMNCCU	Minimum Percent CCU Utilization
SNTNAF	NAFPCNBU	Percent NCP Buffer Util.
SNTNAF	NAFMXNBU	Max. Percent NCP Buffer Util.
SNTNAF	NAFMNNBU	Min. Percent NCP Buffer Util.
SNTNAF	NAFPCTIS	Percent Time in Slowdown

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTPSU	PSUBRESC	Response Event Count (Both)
SNTPSU	PSUNRFMR	Number Text Bytes Received
SNTPSU	PSUNRFMS	Number Text Bytes Sent
SNTPSU	PSUNRNFR	Number Control Bytes Received
SNTPSU	PSUNRMFS	Number Control Bytes Sent
SNTPSU	PSUNRPFR	Number Text PIUs Received
SNTPSU	PSUNRPFS	Number Text PIUs Sent
SNTPSU	PSUNRPNR	Number Control PIUs Received
SNTPSU	PSUNRPNS	Number Control PIUs Sent
SNTPSU	PSUNRMBR	No. of Text Message Bytes Rec'd
SNTPSU	PSUNRMBS	No. of Text Message Bytes Sent
SNTPSU	PSUNRMSR	No. of Text Messages Rec'd
SNTPSU	PSUNRMSS	No. of Text Messages Sent
SNTPSU	PSUMXMBR	Max Text Message Rec'd
SNTPSU	PSUMXMBS	Max Text Message Sent
SNTPSU	PSUMXTBR	Max Text PIU Rec'd
SNTPSU	PSUMXTBS	Max Text PIU Sent
SNTPSU	PSUAVNTM	Average Network Response Time
SNTPSU	PSUAVHTM	Average Host Response Time
SNTPSU	PSUAVTTM	Average Total Response Time
SNTPSU	PSUBRESC	Response Event Count (Both)
SNTPSU	PSUPCBR1	Cum. Pct Both Resp Within Limit 1
SNTPSU	PSUPCBR2	Cum. Pct Both Resp Within Limit 2
SNTPSU	PSUPCBR3	Cum. Pct Both Resp Within Limit 3
SNTPSU	PSUPCBR4	Cum. Pct Both Resp Within Limit 4
SNTPSU	PSUPCHR1	Cum. Pct Host Resp Within Limit 1
SNTPSU	PSUPCHR2	Cum. Pct Host Resp Within Limit 2
SNTPSU	PSUPCHR3	Cum. Pct Host Resp Within Limit 3
SNTPSU	PSUPCHR4	Cum. Pct Host Resp Within Limit 4
SNTPSU	PSUPCTR1	Cum. Pct Total Resp Within Limit 1
SNTPSU	PSUPCTR2	Cum. Pct Total Resp Within Limit 2

SNTPSU	PSUPCTR3	Cum. Pct Total Resp Within Limit 3
SNTPSU	PSUPCNON	Pct of Total Events W/out Netwk Resp
SNTPSU	PSUTDST1	Response Distribution Count 1 (Total)
SNTPSU	PSUTDST2	Response Distribution Count 2 (Total)
SNTPSU	PSUTDST3	Response Distribution Count 3 (Total)
SNTPSU	PSUTDST4	Response Distribution Count 4 (Total)
SNTPSU	PSUTDST5	Response Distribution Count 5 (Total)
SNTPSU	PSUMXHTM	Maximum Host Resp Time
SNTPSU	PSUMXNTM	Maximum Net Resp Time (w/ Host Tx)
SNTPSU	PSUMXTTM	Maximum Total Resp Time
SNTPSU	PSUERQTM	Total Time Exceeded Squared
SNTPSU	PSUERTTM	Total Time Oper Threshold Exceeded
SNTPSU	PSUHRQTM	Host Response Time Squared
SNTPSU	PSUNNHTM	Network Response Time
SNTPSU	PSUNRHO	Number of Host Only Transactions
SNTPSU	PSUNRNNH	Resp Event Count (Net)
SNTPSU	PSUNRQTM	Net Response Time Squared (w/ Host Tx)
SNTPSU	PSUORQTM	Net Resp Time Squared
SNTPSU	PSUTRQTM	Total Resp Time Squared
SNTPSU	PSUMXNNH	Maximum Network Resp Time

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTPSY	PSYBRES	Response Event Count (Both)
SNTPSY	PSYNRFMR	Number Text Bytes Received
SNTPSY	PSYNRFMS	Number Text Bytes Sent
SNTPSY	PSYNRNFR	Number Control Bytes Received
SNTPSY	PSYNRMFS	Number Control Bytes Sent
SNTPSY	PSYNRPFR	Number Text PIUs Received
SNTPSY	PSYNRPFS	Number Text PIUs Sent
SNTPSY	PSYNRPNR	Number Control PIUs Received
SNTPSY	PSYNRPNS	Number Control PIUs Sent
SNTPSY	PSYNRHO	Number of Host Only Transactions
SNTPSY	PSYNRMBR	No. of Text Message Bytes Rec'd
SNTPSY	PSYNRMBS	No. of Text Message Bytes Sent
SNTPSY	PSYNRMSR	No. of Text Messages Rec'd
SNTPSY	PSYNRMSS	No. of Text Messages Sent
SNTPSY	PSYMXMBR	Max Text Message Rec'd
SNTPSY	PSYMXMBS	Max Text Message Sent
SNTPSY	PSYMXTBR	Max Text PIU Rec'd
SNTPSY	PSYMXTBS	Max Text PIU Sent
SNTPSY	PSYAVNTM	Average Network Response Time
SNTPSY	PSYAVHTM	Average Host Response Time
SNTPSY	PSYAVTTM	Average Total Response Time
SNTPSY	PSYBRES	Response Event Count (Both)
SNTPSY	PSYPCBR1	Cum. Pct Both Resp Within Limit 1
SNTPSY	PSYPCBR2	Cum. Pct Both Resp Within Limit 2
SNTPSY	PSYPCBR3	Cum. Pct Both Resp Within Limit 3
SNTPSY	PSYPCBR4	Cum. Pct Both Resp Within Limit 4

SNTPSY	PSYPCHR1	Cum. Pct Host Resp Within Limit 1
SNTPSY	PSYPCHR2	Cum. Pct Host Resp Within Limit 2
SNTPSY	PSYPCHR3	Cum. Pct Host Resp Within Limit 3
SNTPSY	PSYPCHR4	Cum. Pct Host Resp Within Limit 4
SNTPSY	PSYPCTR1	Cum. Pct Total Resp Within Limit 1
SNTPSY	PSYPCTR2	Cum. Pct Total Resp Within Limit 2
SNTPSY	PSYPCTR3	Cum. Pct Total Resp Within Limit 3
SNTPSY	PSYPCNON	Pct of Total Events W/out Netwk Resp
SNTPSY	PSYTDST1	Response Distribution Count 1 (Total)
SNTPSY	PSYTDST2	Response Distribution Count 2 (Total)
SNTPSY	PSYTDST3	Response Distribution Count 3 (Total)
SNTPSY	PSYTDST4	Response Distribution Count 4 (Total)
SNTPSY	PSYTDST5	Response Distribution Count 5 (Total)
SNTPSY	PSYMXHTM	Maximum Host Resp Time
SNTPSY	PSYMXNTM	Maximum Net Resp Time (w/ Host Tx)
SNTPSY	PSYMXTTM	Maximum Total Resp Time
SNTPSY	PSYERQTM	Total Time Exceeded Squared
SNTPSY	PSYERTTM	Total Time Oper Threshold Exceeded
SNTPSY	PSYHRQTM	Host Response Time Squared
SNTPSY	PSYNNHTM	Net Resp Time
SNTPSY	PSYNNNH	Resp Event Count (Net)
SNTPSY	PSYNRQTM	Net Response Time Squared (w/ Host Tx)
SNTPSY	PSYORQTM	Net Response Time Squared
SNTPSY	PSYTRQTM	Total Resp Time Squared
SNTPSY	PSYMXNNH	Maximum Network Resp Time

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNPL	NPLBRES	Response Event Count (Both)
SNTNPL	NPLNRFMR	Number Text Bytes Received
SNTNPL	NPLNRFMS	Number Text Bytes Sent
SNTNPL	NPLNRNFR	Number Control Bytes Received
SNTNPL	NPLNRMFS	Number Control Bytes Sent
SNTNPL	NPLNRPFR	Number Text PIUs Received
SNTNPL	NPLNRPFS	Number Text PIUs Sent
SNTNPL	NPLNRPNR	Number Control PIUs Received
SNTNPL	NPLNRPNS	Number Control PIUs Sent
SNTNPL	NPLNRMBR	No. of Text Message Bytes Rec'd
SNTNPL	NPLNRMBS	No. of Text Message Bytes Sent
SNTNPL	NPLNRMSR	No. of Text Messages Rec'd
SNTNPL	NPLNRMSS	No. of Text Messages Sent
SNTNPL	NPLMXMBR	Max Text Message Rec'd
SNTNPL	NPLMXMBS	Max Text Message Sent
SNTNPL	NPLMXTBR	Max Text PIU Rec'd
SNTNPL	NPLMXTBS	Max Text PIU Sent
SNTNPL	NPLAVNTM	Average Network Response Time
SNTNPL	NPLAVHTM	Average Host Response Time
SNTNPL	NPLAVTTM	Average Total Response Time
SNTNPL	NPLBRES	Response Event Count (Both)

SNTNPL	NPLPCBR1	Cum. Pct Both Resp Within Limit 1
SNTNPL	NPLPCBR2	Cum. Pct Both Resp Within Limit 2
SNTNPL	NPLPCBR3	Cum. Pct Both Resp Within Limit 3
SNTNPL	NPLPCBR4	Cum. Pct Both Resp Within Limit 4
SNTNPL	NPLPCHR1	Cum. Pct Host Resp Within Limit 1
SNTNPL	NPLPCHR2	Cum. Pct Host Resp Within Limit 2
SNTNPL	NPLPCHR3	Cum. Pct Host Resp Within Limit 3
SNTNPL	NPLPCHR4	Cum. Pct Host Resp Within Limit 4
SNTNPL	NPLPCTR1	Cum. Pct Total Resp Within Limit 1
SNTNPL	NPLPCTR2	Cum. Pct Total Resp Within Limit 2
SNTNPL	NPLPCTR3	Cum. Pct Total Resp Within Limit 3
SNTNPL	NPLPCNON	Pct of Total Events W/out Netwk Resp
SNTNPL	NPLTDST1	Response Distribution Count 1 (Total)
SNTNPL	NPLTDST2	Response Distribution Count 2 (Total)
SNTNPL	NPLTDST3	Response Distribution Count 3 (Total)
SNTNPL	NPLTDST4	Response Distribution Count 4 (Total)
SNTNPL	NPLTDST5	Response Distribution Count 5 (Total)
SNTNPL	NPLMXHTM	Maximum Host Resp Time
SNTNPL	NPLMXNTM	Maximum Net Resp Time (w/ Host Tx)
SNTNPL	NPLMXTTM	Maximum Total Resp Time
SNTNPL	NPLERQTM	Total Time Exceeded Squared
SNTNPL	NPLERTTM	Total Time Oper Threshold Exceeded
SNTNPL	NPLHRQTM	Host Response Time Squared
SNTNPL	NPLNNHTM	Net Resp Time
SNTNPL	NPLNRHO	Number of Host Only Transactions
SNTNPL	NPLNRNNH	Resp Event Count (Net)
SNTNPL	NPLNRQTM	Net Response Time Squared (w/ Host Tx)
SNTNPL	NPLORQTM	Net Resp Time Squared
SNTNPL	NPLTRQTM	Total Resp Time Squared
SNTNPL	NPLMXNNH	Maximum Net Resp Time

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNSV	NSVCOS	Class of Service
SNTNSV	NSVPCOBJ	Objective Percentage
SNTNSV	NSVROBTM	Objective Response Time
SNTNSV	NSVTRESC	Total Response Event Count
SNTNSV	NSVAVTTM	Average Total Response TIme
SNTNSV	NSVPCOBM	Pct of Times Response Obj Met
SNTNSV	NSVPCTR1	Cum. Pct All Response Within Limit 1
SNTNSV	NSVPCTR2	Cum. Pct All Response Within Limit 2
SNTNSV	NSVPCTR3	Cum. Pct All Response Within Limit 3
SNTNSV	NSVPCTR4	Cum. Pct All Response Within Limit 4

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
NVSLSY	LSYNRCBR	Number Control Bytes Received
NVSLSY	LSYNRCBS	Number Control Bytes Sent
NVSLSY	LSYNRCPR	Number Control PIUs Received

NVSLSY	LSYNRCPS	Number Control PIUs Sent
NVSLSY	LSYNRRROM	Number of Times Resp Obj Met
NVSLSY	LSYNRTBR	Number Text Bytes Received
NVSLSY	LSYNRTBS	Number Text Bytes Sent
NVSLSY	LSYNRTPR	Number Text PIUs Received
NVSLSY	LSYNRTPS	Number Text PIUs Sent
NVSLSY	LSYAVTTM	Average Total Response Time
NVSLSY	LSYC0S	Class of Service
NVSLSY	LSYPC0BJ	Objective Percentage
NVSLSY	LSYROBTM	Objective Response Time
NVSLSY	LSYPC0BM	Pct of Times Response Obj Met
NVSLSY	LSYPCTR1	Cum. Pct All Resp Within Limit 1
NVSLSY	LSYPCTR2	Cum. Pct All Resp Within Limit 2
NVSLSY	LSYPCTR3	Cum. Pct All Resp Within Limit 3
NVSLSY	LSYPCTR4	Cum. Pct All Resp Within Limit 4

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
NVSNLL	NLLNRCBR	Number Control Bytes Received
NVSNLL	NLLNRCBS	Number Control Bytes Sent
NVSNLL	NLLNRCPR	Number Control PIUs Received
NVSNLL	NLLNRCPS	Number Control PIUs Sent
NVSNLL	NLLNRRROM	Number of Times Resp Obj Met
NVSNLL	NLLNRTBR	Number Text Bytes Received
NVSNLL	NLLNRTBS	Number Text Bytes Sent
NVSNLL	NLLNRTPR	Number Text PIUs Received
NVSNLL	NLLNRTPS	Number Text PIUs Sent
NVSNLL	NLLAVTTM	Average Total Response Time
NVSNLL	NLLC0S	Class of Service
NVSNLL	NLLPC0BJ	Objective Percentage
NVSNLL	NLLROBTM	Objective Response Time
NVSNLL	NLLPC0BM	Pct of Times Response Obj Met
NVSNLL	NLLPCTR1	Cum. Pct All Resp Within Limit 1
NVSNLL	NLLPCTR2	Cum. Pct All Resp Within Limit 2
NVSNLL	NLLPCTR3	Cum. Pct All Resp Within Limit 3
NVSNLL	NLLPCTR4	Cum. Pct All Resp Within Limit 4

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
NVNSA	NSANRCBR	Number Control Bytes Received
NVNSA	NSANRCBS	Number Control Bytes Sent
NVNSA	NSANRCPR	Number Control PIUs Received
NVNSA	NSANRCPS	Number Control PIUs Sent
NVNSA	NSANRTBR	Number Text Bytes Received
NVNSA	NSANRTBS	Number Text Bytes Sent

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
NVSRTE	RTENRTCH	Total Characters Transmitted

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
NVSRTM	RTMAVTTM	Average Total Response Time
NVSRTM	RTMCNTR	Objective Counter Number
NVSRTM	RTMPCOBJ	Objective Percentage
NVSRTM	RTMROBTM	Objective Response Time
NVSRTM	RTMTRESC	Total Response Event Count
NVSRTM	RTMPCOBM	Pct of Times Response Obj Met
NVSRTM	RTMPCTR1	Cum. Pct All Resp Within Limit 1
NVSRTM	RTMPCTR2	Cum. Pct All Resp Within Limit 2
NVSRTM	RTMPCTR3	Cum. Pct All Resp Within Limit 3
NVSRTM	RTMPCTR4	Cum. Pct All Resp Within Limit 4
FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNSP	NSPAVHTM	Average Host Response Time
SNTNSP	NSPAVNTM	Average Network Response Time
SNTNSP	NSPAVTTM	Average Total Response Time
SNTNSP	NSPCNRTM	Network Response Time (Computed)
SNTNSP	NSPHRSTM	Host Response Time
SNTNSP	NSPLHRTM	Last Host Response Time
SNTNSP	NSPLNRTM	Last Network Response Time
SNTNSP	NSPMXHTM	Maximum Host Response Time
SNTNSP	NSPMXNTM	Maximum Network Response Time
SNTNSP	NSPNRBYR	Cumulative Bytes Received
SNTNSP	NSPNRBYS	Cumulative Bytes Sent
SNTNSP	NSPNRESC	Network Responses
SNTNSP	NSPNROUT	Number of Outputs
SNTNSP	NSPNRSTM	Network Response Time (Measured)
SNTNSP	NSPPCTR1	Cum. Pct Total Resp Within Limit 1
SNTNSP	NSPPCTR2	Cum. Pct Total Resp Within Limit 2
SNTNSP	NSPPCTR3	Cum. Pct Total Resp Within Limit 3
SNTNSP	NSPPCTR4	Cum. Pct Total Resp Within Limit 4
SNTNSP	NSPRDST1	Response Distribution Count 1
SNTNSP	NSPRDST2	Response Distribution Count 2
SNTNSP	NSPRDST3	Response Distribution Count 3
SNTNSP	NSPRDST4	Response Distribution Count 4
SNTNSP	NSPRDST5	Response Distribution Count 5
SNTNSP	NSPRVAL1	Response Distribution Limit 1
SNTNSP	NSPRVAL2	Response Distribution Limit 2
SNTNSP	NSPRVAL3	Response Distribution Limit 3
SNTNSP	NSPRVAL4	Response Distribution Limit 4
SNTNSP	NSPTRESC	Number of Responses
SNTNSP	NSPNRTXS	Number of Transactions (# of Inputs)
SNTNSP	NSPTRSTM	Total Response Time
SNTNSP	NSPNRTRI	Number of Transactions (LU62 Sessions)
SNTNSP	NSPNRURM	Total User Responses Measured (LU62)

FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNSS	NSSAVHTM	Average Host Response Time
SNTNSS	NSSAVNTM	Average Network Response Time
SNTNSS	NSSAVTTM	Average Total Response Time
SNTNSS	NSSCNRTM	Network Response Time (Computed)
SNTNSS	NSSHRSTM	Host Response Time
SNTNSS	NSSLHRTM	Last Host Response Time
SNTNSS	NSSLNRTM	Last Network Response Time
SNTNSS	NSSMXHTM	Maximum Host Response Time
SNTNSS	NSSMXNTM	Maximum Network Response Time
SNTNSS	NSSNRBYR	Cumulative Bytes Received
SNTNSS	NSSNRBYS	Cumulative Bytes Sent
SNTNSS	NSSNRBYT	Cumulative Bytes Transmitted
SNTNSS	NSSNRESC	Network Responses
SNTNSS	NSSNROUT	Number of Outputs
SNTNSS	NSSNRSTM	Network Response Time (Measured)
SNTNSS	NSSPCTR1	Cum. Pct Total Resp Within Limit 1
SNTNSS	NSSPCTR2	Cum. Pct Total Resp Within Limit 2
SNTNSS	NSSPCTR3	Cum. Pct Total Resp Within Limit 3
SNTNSS	NSSPCTR4	Cum. Pct Total Resp Within Limit 4
SNTNSS	NSSRDST1	Response Distribution Count 1
SNTNSS	NSSRDST2	Response Distribution Count 2
SNTNSS	NSSRDST3	Response Distribution Count 3
SNTNSS	NSSRDST4	Response Distribution Count 4
SNTNSS	NSSRDST5	Response Distribution Count 5
SNTNSS	NSSRVAL1	Response Distribution Limit 1
SNTNSS	NSSRVAL2	Response Distribution Limit 2
SNTNSS	NSSRVAL3	Response Distribution Limit 3
SNTNSS	NSSRVAL4	Response Distribution Limit 4
SNTNSS	NSSTRESC	Number of Responses
SNTNSS	NSSNRTXS	Number of Transactions (# of Inputs)
SNTNSS	NSSSTRSTM	Total Response Time
SNTNSS	NSSNRTRI	Number of Transactions (LU62 Sessions)
SNTNSS	NSSNRURM	Total User Responses Measured (LU62)
FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNVR	NVRNRBYS	Cumulative Bytes Sent
SNTNVR	NVRNRMOP	Measured Outbound PIU's
SNTNVR	NVRNRTOP	Total Outbound PIU's
SNTNVR	NVRAVPL	Average Outbound PIU Length
SNTNVR	NVRNRESC	Network Responses (Measured)
FILE	ELEMENT	DESCRIPTION
-----	-----	-----
SNTNAC	NACNRCBR	Number Control Bytes Received
SNTNAC	NACNRCBS	Number Control Bytes Sent
SNTNAC	NACNRCPR	Number Control PIUs Received

SNTNAC	NACNRCPS	Number Control PIUs Sent
SNTNAC	NACNRTBR	Number Text Bytes Received
SNTNAC	NACNRTBS	Number Text Bytes Sent
SNTNAC	NACNRTBY	Total Number of Bytes Transmitted
SNTNAC	NACNRTPI	Total Number of PIUs Transmitted
SNTNAC	NACNRTPR	Number Text PIUs Received
SNTNAC	NACNRTPS	Number Text PIUs Sent

2.3.4.3.2 Performance Management Exceptions

The standard exceptions listed below may be used for analyzing network performance. The objectives indicate that performance objectives have been missed or that conditions have occurred that may contribute to missed performance objectives. The exception reporting provided with this product is discussed in Chapter 4. Detailed descriptions are provided for each exception.

- o 12001 - Link Average Utilization Threshold Exceeded
- o 12002 - Link Error Count Threshold Exceeded
- o 12003 - Link Resource Outbound Queue Length Exceeded
- o 12004 - Link Polling Rate Below Threshold
- o 12005 - Link Positive Polling Percentage Threshold Exceeded
- o 12061 - Network Component Error Threshold Exceeded
- o 12062 - Component Resource Outbound Q Length Exceeded
- o 12121 - 37XX Utilization Threshold Exceed
- o 12122 - Percentage CCU Time in Slowdown Threshold Exceeded
- o 12123 - Average Free Buffer Queue Length Below Limit
- o 12124 - Avg NCP Channel Hold Q Length Threshold Exceeded
- o 12181 - Network Component Traffic Exceeds Limit
- o 12182 - Network Component Traffic Below Minimum
- o 12183 - Network Component Error Rate Exceeds Limit
- o 12184 - NCP Processor Overloaded
- o 12185 - NCP Processor Under-utilized
- o 12186 - Negative Poll Rate Exceeds Limit
- o 12187 - Positive Poll Rate Below Limit
- o 12188 - Messages Per Minute Exceeds Limit
- o 12189 - Bytes Per Second Exceeds Limit
- o 12190 - Percentage of Free Buffers Below Minimum
- o 12191 - Outbound Queue Length Exceeds Limit
- o 12192 - Percentage of Time in Slowdown Exceeds Limit
- o 12193 - Percentage of Bytes Retransmitted Exceeds Limit
- o 12194 - Percentage of NCP Buffers Used Exceeds Limit
- o 12301 - Response Objective Missed For Performance Cls
- o 12541 - NPDA Event
- o 12542 - NPDA Event Alert
- o 12601 - NPDA Statistical Alert
- o 12661 - Host Response Outside Bounds-Count Exceeded for SLU
- o 12662 - Net Response Outside Bounds-Count Exceeded for SLU
- o 12663 - Total Response Outside Bounds-Count Exceeded for SLU
- o 12780 - Host Response Outside Bounds-Count Exceeded

- for Link
- o 12781 - Net Response Outside Bounds-Count Exceeded
for Link
- o 12782 - Total Response Outside Bounds-Count Exceeded
for Link
- o 12801 - Response Objective Missed for APPL/PCLASS
- o 12802 - Response Objective Missed for LINK/PCLASS

2.3.4.3.3 Performance Management Reports

The standard reports listed below can be used when managing network performance. These reports are described in Chapter 3.

TABULAR REPORTS

- o SNT101 - NPM Service by Application Report
- o SNT103 - NPM Service by Link Report
- o SNT105 - NLDM Service by Performance Class Report
- o SNT111 - NLDM Service by Application
- o SNT112 - NLDM Service by Link
- o SNT113 - NLDM Service by Control Unit
- o SNT114 - NLDM Service by Terminal
- o SNT115 - NLDM Service by Performance Class
- o SNT121 - CA NetSpy Service by Application
- o SNT122 - CA NetSpy Service by Terminal
- o SNT201 - NPM Workload by Application Report
- o SNT203 - NPM Workload by Link Report
- o SNT208 - NPM/NetSpy Utilization by NCP Report
- o SNT209 - NPM/NetSpy NCP Workload by Link Report
- o SNT211 - NLDM Workload by Application
- o SNT212 - NLDM Workload by Link
- o SNT213 - NLDM Workload by Control Unit
- o SNT214 - NLDM Workload by Terminal
- o SNT215 - NPM/NetSpy NCP Workload by Link Report
- o SNT216 - NPM/NetSpy NCP Workload by Link Report
- o SNT221 - CA NetSpy Workload by Application
- o SNT222 - CA NetSpy Workload by Terminal
- o SNT401 - NPM NCP Data Collection Report
- o SNT401 - CA NetSpy NCP Data Collection Report
- o SNT403 - NPM Session Data Collection Report
- o SNT601 - NPDA Event Analysis Report
- o SNT602 - NPDA Statistics Analysis Report

GRAPHIC INQUIRIES

- o SNTG101 - Average Response by Performance Class
- o SNTG102 - Application Service Analysis
- o SNTG103 - Application Service Analysis by Hour
- o SNTG201 - Traffic Profile Report for Link
- o SNTG202 - Communications Controller Utilization Profile
- o SNTG203 - NCP Buffer Utilization Trend
- o SNTG204 - Percent Link Utilization by Zone
- o SNTG301 - Error Count for Link

- o SNTG302 - Percent Temporary Errors to Traffic
- o SNTG303 - NPDA Events for Cluster Controller

MICF INQUIRIES

- o SNTCD1 NetView Daily Avg Resp by PCLASS
- o SNTCD4 NetView Daily % Resp Within Obj by PCLASS
- o SNTCDI NetView Daily Avg Response by Link
- o SNTCDN NetView Daily % Resp Within Obj. by Link
- o SNTCD5 CA NetSpy Daily PLU Resp Time Components
- o SNTCDT CA NetSpy Daily SLU Resp Time Components
- o SNTCD6 NPM Daily Pct. NCP Cycle Util.
- o SNTCD7 NPM Daily NCP Buffer Utilization
- o SNTCD8 NPM Daily Link Utilization
- o SNTCDP CA NetSpy Daily Pct. NCP Cycle Util.
- o SNTCDQ CA NetSpy Daily NCP Buffer Utilization
- o SNTCDR CA NetSpy Daily Link Utilization
- o SNTCDZ CA NetSpy Daily % Time VR Held/Blocked
- o SNTCD5 CA NetSpy Daily Avg VR Response Time
- o SNTCDD NetView Daily Chars/1000 by SNTACT1
- o SNTCDE NetView Daily Chars/1000 by VR
- o SNTCDF NetView Daily Data Chars/1000 by SNTACT1
- o SNTCDG NetView Daily Cntl Chars/1000 by SNTACT1
- o SNTLDA NetView Application Service/Workload Ranking
- o SNTLD0 NPM Application Service/Workload Ranking
- o SNTLD2 CA NetSpy Application Service/Workload Ranking
- o SNTLDX NPM/NetSpy Daily Link Ranking by Zone
- o SNTLDY NPM/NetSpy Daily Link Ranking by Hour
- o SNTCDX NSA/NGA Daily Data Chars/1000 by SNTACT1
- o SNTCDY NSA/NGA Daily Data PIU Traffic by SNTACT1

Note that any report listed above that begins with the name of the data source NetView NLDM can also be produced from equivalent data collected by CA NetMaster NTS. Any report beginning with the name of the data source NPDA can also be produced from equivalent data collected by CA NetMaster NEWS.

2.3.4.3.4 Performance Analysis

One of the most significant components of network response time is the delay between the time you press ENTER on the terminal and polling of the terminal. This delay is called "wait for poll." The length of the wait for a poll is a function of the polling rate of the line and the number of terminals that have outstanding requests for service.

These effects can be seen in the following example:

Assume that there are two cluster controllers (SNA PUs) on a peripheral link. Each controller has fifteen 3270 devices attached to it. The link polling rate is twenty polls per second. If, on the average, two-thirds of the terminals have outstanding requests at any one time, each terminal will be polled approximately once a second (ignoring any data transmission time). In this case, network response time would always be greater than one second.

From this example, it is clear that a low polling rate can significantly affect response time, but a high polling rate also effects negatively on response time. High polling rates cause communications control unit utilizations to increase out of proportion to the amount of data transferred. It requires many more CCU instructions to generate a given level of link utilization through polling than to generate the same utilization level through data transmission.

Neither NetView Session Monitor/NLDM nor NPM nor CA NetSpy measures the response delay incurred by wait for poll; therefore, the choice of a polling rate for a line must be made somewhat by trial and error. As a rule of thumb, a link should be polled at least once per second per active device. The adequacy of the polling rate can then be judged based on the percentage of positive and negative polls. The optimum positive and negative poll percentages can be judged based on the average time between end-user commands (user think time). If there are twenty terminals on a link that is being polled twenty times a second and the average user think time is twenty seconds, there should be at least one outstanding request every second; so that one poll, or five percent of the total, would be positively acknowledged.

Polling statistics are displayed on the NCP Utilization by Link report that is described in Section 3.1.3.2.4.

2.4 Specialized Analysis

This section describes analyses you can perform using the data from the CA MICS Network Analyzer Option's files.

Estimating Backbone Network Communications Capacity:

Background

The communications controller subarea nodes that are channel-attached to host processors and the links that interconnect them make up what is loosely termed the "backbone" of a network. It is through these communications controllers and their associated links that the bulk of the network traffic (to and from the mainframe applications) ultimately flows. This concentration of load means that inadequate capacity in the network usually occurs first in the backbone.

Obviously, any significant increase in overall network load will affect the backbone elements, but normal network maintenance can significantly affect the backbone's load carrying capacity. In some cases, relatively minor NCP generation parameter changes can have drastic effects on the utilization level of communications control units (CCUs). This is because small changes to buffer lengths or negative poll delays can greatly increase the average number of CCU processor instructions required to transmit a byte of data.

Methodology

One way to quantify the effects of NCP gen changes is to track the mean instruction path length-per-byte of data passed through each CCU. The mean instruction path length varies with the traffic mix but is relatively invariant under load. Therefore it is unnecessary to ensure that exactly the same load exists on the processor as long as the traffic mix is the same. To ensure that the mix is homogeneous, observe the following rules of thumb:

- o Always compare path length measurements from the same times in the processing day.
- o Always compare the same days in the processing cycle (for example, month-end to month-end).

- o Avoid comparisons where new applications have been added unless you have verified that the new applications do not change the traffic mix. (Refer to Application below.)

Determine the total amount of traffic passing through a CCU during the period of interest. This can be done by summarizing the Number of Bytes Sent (CAFNRCHS) and Number of Bytes Received (CAFNRCHR) fields from the SNTCAF File for the particular CCU and time period of interest.

Determine the number of instructions executed by the processor in the CCU during that time period by multiplying the processor instruction rate by the length of the time period of interest.

Divide the total number of instructions available by the number of characters passed to obtain the mean instruction path length per byte. This number is the approximate number of processor instructions required to move a byte of data through the CCU and is generally on the order of 100 instructions per byte.

To be rigorous, the number of instructions lost due to cycle stealing should be calculated. These cycles cannot be used by the processor because Type 2 and 3 channel adapters preempt it to transfer data to and from storage. The number of stolen cycles can be calculated by estimating the number of bytes transferred to and from the channel adapter (CA) and multiplying them by the number of cycles the CA requires to transfer a byte of data. The total number of stolen cycles are then subtracted from the total number available before dividing by the total traffic. In practice, this adjustment is generally very small.

Application

Because the mean path length-per-byte is largely sensitive to traffic mix only (for a given set of NCP gen parameters) it can be used to estimate the capacity of a CCU handling that traffic mix. That is, the data handling capacity of a CCU per unit time will be approximately the CCU's processor instruction capacity-per-unit-time divided by the mean instruction path length-per-byte. This estimate has been shown to be surprisingly robust in widely varying environments.

Often estimates of capacity are made by assuming that traffic generated by a new application will place much the same load on the network backbone that existing traffic does. That is, that the mix of the new application's traffic is the same as the mix of the existing applications' traffic. By isolating the new application in a test environment and computing the mean instruction path length-per-byte, the validity of this assumption can be tested.

Before and after comparisons of the mean instruction path, length-per-byte should be made for each new NCPGEN. This comparison will quantify the cost in backbone capacity of supporting new facilities or, conversely, the benefits derived from NCP tuning. Most importantly, it will prevent the network analyst, who is removed from the day-to-day NCP gen process, from being surprised by an unexpected reduction in backbone capacity.

Basic Network Accounting Background

Historically, billing for network resources has been largely relegated to the few adventurous organizations that dared to experiment. Now, the information in the CA MICS Network Analyzer Option and the billing facilities of the CA MICS Accounting and Chargeback Option can be combined to offer a network accounting approach that will satisfy the basic requirements of many enterprises.

Basic network accounting is supported for multiple information sources: CA NetSpy terminal data, and network session accounting data/network gateway accounting data, Tivoli NetView Performance Monitor (NPM) session data, NPM network session accounting/network gateway accounting data, NetView Session Monitor Response Time Monitor (RTM) data,

NetView Session Monitor accounting and availability data, CA NetMaster RTM data and accounting data. Since there is an overlap in information provided by these sources, the decision on which sources to use is governed by the needs of the enterprise, the specific information available from each source, and the operational costs associated with each network monitor.

Since more than one network monitor can collect data for the same session, it is possible for you to develop a billing scheme that causes duplicate billing for some sessions. For example, if you are billing for session connect time or characters transmitted based on information from both NPM and NetView, you can end up billing some users twice for the same session activity. You should carefully evaluate these considerations when constructing a billing scheme based on network monitor data from more than one source.

Billing is supported for connectivity to specific network resources, session duration, and character traffic for terminals or groups of terminals in session with specific applications. A differential charge can be assessed for different classes of service, local or remote attachment, transmission priority, explicit route, virtual route, or any of several other service or configuration related factors.

Accounting Information Sources

The basic network accounting approach supported by the CA MICS Network Analyzer Option and the CA MICS Accounting and Chargeback Option uses data from the following information sources:

- o CA NetSpy Network Session Accounting
- o CA NetSpy Network Gateway Accounting
- o CA NetSpy VTAM Interface: Terminal Activity
- o Network Performance Monitor (NPM) Session
- o NPM Network Session Accounting
- o NPM Network Gateway Accounting
- o NetView Session Monitor Response Time Monitor
- o NetView Session Monitor Accounting and Availability
- o CA NetMaster NTS Response Time Monitor
- o CA NetMaster NTS Accounting

These sources provide different views of the data and permit different ways of performing network accounting. There are six CA MICS files that contain data from these sources, and which can be used for accounting:

- o NCP Network Accounting (SNTNAC) File
- o CA NetSpy Terminal (SNTNSS) File
- o NPM User Activity (SNTPSU) File
- o NLDM Session Accounting (NVSNSA) File
- o NLDM Session Connectivity (NVSNSC) File
- o NLDM Response Time (NVSRTM) File

Each of these files is described in Chapter 5, along with a list of the data elements associated with each file. See Appendix B for a description of specific data elements and their use within each file. This overview should help you to select the information appropriate to your billing needs.

Differential Billing

A standard requirement for resource billing is differential charging based on service or configuration.

The user with a locally-attached terminal can be charged a premium versus the user with a remotely-attached device since the locally-attached terminal provides faster response time. Or, based on the additional cost of the facilities for a remotely-attached user, the differential can be applied in exactly the opposite way.

To accommodate this requirement, logical unit-to-logical unit (LU-LU) sessions are distinguished as local, remote, or application-to-application (APPL-APPL) by the CA MICS Network Analyzer Option. Other session types (for example, system services control point to system services control point (SSCP to SSCP)) are designated as "other." Users of the CA MICS Accounting and Chargeback Option can, through a special feature called XMITTYPE, set different rates for each billable element depending on whether the session is local, remote, or APPL-APPL. For example, the cost for locally-attached devices could be set at \$.04 per thousand characters, while the cost for remotely-attached devices could be set at \$.02 per thousand characters.

The method used by CA MICS to distinguish local, remote, and APPL-APPL sessions is described later in this section. If you choose this billing approach, be sure to read this section before you finish installing the CA MICS Network Analyzer Option.

In addition to this facility, CA MICS provides for

differential billing based on other service and configuration considerations. For example, this capability could be useful for an enterprise that assigns a surcharge to network traffic with a higher priority, and therefore faster service.

One way to assign different priorities to different types of work in a network is to use transmission priorities. Transmission priorities can be assigned to different classes of work so that, for example, interactive traffic receives a higher priority than batch traffic. Transmission priority values of 0, 1, and 2 can be assigned, with 2 representing the highest priority.

In the example where interactive and batch are assigned different priorities, you can assign to interactive the highest priority of 2, and to batch the lowest priority of 0. You can apply a factor to charges for interactive traffic that result in their cost per thousand characters being 1.5 times the standard cost, which is applied to batch traffic. The way to implement such a billing strategy using the CA MICS Network Analyzer Option is through the Network Service Group facility (NETGROUP) described in Section 7.3 of this guide.

Identifying Local Versus Remote Sessions (ffflDEV)

Because most CA MICS Network Analyzer Option data sources (excluding NPM) do not identify sessions as local or remote, CA MICS determines this information from the data available. The approach taken is to compare primary to secondary subarea identifiers (NPM) and primary and secondary subarea physical unit identifiers (NetView and CA NetMaster). When the identifiers are equal, the session is considered to be a local session. When the identifiers are unequal, the session is considered to be a remote session.

As an exception, to account for logical unit-to-logical unit (LU-LU) sessions in which the secondary logical unit (SLU) is an application, you can designate a list of applications that can participate in APPL-APPL sessions by coding the application names in prefix.MICS.PARMS(NETAPPL). The CA MICS Network Analyzer Option identifies any session whose SLU is found in the NETAPPL table as an APPL-APPL session. NETAPPL is described in Chapter 7. Sessions that are not LU-LU, such as system services control point to physical unit (SSCP-PU) sessions, are identified as "other" sessions.

A local device flag data element is set to indicate local

(L), remote (R), APPL-APPL (A), or other (O) in these files:

- o SNTNAC file (NACLDEV)
- o SNTPSU file (PSULDEV)
- o SNTNSS file (NSSLDEV)
- o NVSNSC file (NSCLDEV)

2.5 Data Manipulation Guidelines

This section describes different interpretations of the data collected by Tivoli NPM, NetView Session Monitor/NLDM, NetView Hardware Monitor/NPDA, CA NetMaster, and CA NetSpy that may affect the usability of the data.

Tivoli NPM and CA NetSpy

- o Comparison of application monitor (for example, CA TSO/MON PM), NPM, and CA NetSpy host response times.

Tivoli NPM and CA NetSpy include VTAM processing time and operating system time as part of host response time. Application monitors start timing when they receive a request from VTAM and stop timing when they return the response to VTAM. Therefore, host response time as measured by either NPM or CA NetSpy should be greater than that measured by an application monitor by the amount of VTAM processing time plus the operating system overhead incurred by VTAM. In other words, VTAM delay can be approximated by subtracting the application monitor response time from the NPM or CA NetSpy response time for the same traffic.

- o Accuracy of response time measurements.

Both Tivoli NPM and CA NetSpy assume that the time for a terminal to return a definite response approximates the time an input message takes to reach VTAM through the network. Tivoli indicates that this is true for single request/response unit transactions only. However, it seems reasonable that the complexity of the route and the rate of variance of overall network queuing delay will also affect the accuracy of this number. In other words, the more network elements (links and nodes) through which a transaction passes, the more likely that the magnitude of the NPM or CA NetSpy response time error is increased. However, since this is just as likely to be underestimated as overestimated, analysis of a significant sample of data should closely approximate the actual response time.

NetView/NLDM CA NetMaster and the 3274/3174 Response Time Monitor (RTM)

- o Accuracy of response time measurements.

Response time as measured by the 3274/3174 Response Time Monitor (RTM) in conjunction with either NetView Session Monitor/NLDM or CA NetMaster may be inaccurate in environments that use non-IBM hardware to link the terminal and the 3274 control unit. For example, significant delay that is not measured by either NetView Session Monitor/NLDM or CA NetMaster could be imposed on an end-user if a local area network installation accesses a 3274 as a LAN gateway. The RTM does not measure the time required to transfer data from the 3274/3174 control unit to the terminal. A bottleneck in the 3274/3174 at this time can cause a significant delay. Because the use of LANs is rapidly increasing, you should keep this potential source of error in mind.

- o Variation of response time measurements with response definitions.

NetView Session Monitor/NLDM allows the data center to select the definition for the end of a transaction for the purpose of response timing. This definition may be any of the following:

- o Receiving the first byte of the outgoing message
- o Receiving a keyboard unlock
- o Changing direction/ending bracket protocol
- o Time to last character

Using the First Byte definition:

This definition ignores the network transmission time for all but the first character of the message. Frequently network transmission time represents the largest portion of response time.

Using the Keyboard Unlock definition:

If there are multiple outbound (transmission to terminal) messages for each transaction, all requesting definite response, this definition ignores the network response time for all messages after the first definite response.

NetView Hardware Monitor/NPDA and CA NetMaster NEWS

- o Cross-domain Recording Considerations

Both NetView Hardware Monitor and CA NetMaster NEWS reliability data may be collected from multiple network domains and stored in the same network database.

A single resource accessed by two separate domains (for example, network resources linked to both domains at different times) may have statistics, events, and alerts recorded under different symbolic names and identified as being attached to different higher-level resources. You must take this into account when analyzing data in the SNTNEF and SNTNSF Files.

2.6 Multiple Session Manager Considerations

A multiple session manager is a VTAM application that permits a terminal user to maintain active sessions with more than one host application simultaneously. The key advantage of such a product is that it eliminates the need for a user who requires access to two or more host applications to log off of one application and log on to the other. This in turn reduces system resources for application logons and enhances end user productivity.

Examples of multiple session managers are:

- o CA TPX Session Management for z/OS
- o CA Teleview Session Management for z/OS
- o SOLVE: Access
- o NetView Access, Tivoli

While each multiple session manager is implemented differently, there are specific data-related issues that are common among them.

A multiple session manager introduces a separate layer in the interface between the user and the host application. The multiple session manager layer controls the user's access to 16 to 255 separate applications, depending upon the product's implementation. Figure 2-15, Multiple Session Manager User Session, illustrates the interface between the user at a terminal, the multiple session manager, and the host applications.

The terminal user is identified to the multiple session manager by a userid/password. Once logged on to the multiple session manager, the user may initiate sessions with authorized host applications. For example, in Figure 2-15, the user may log on to TSO and CICS. Once logged on to these applications, the user may switch at will between them without having to log off of one before logging on to the other.

To accomplish this, the multiple session manager establishes three separate sessions, as illustrated in Figure 2-15. First, there is a session between the user's terminal and the multiple session manager. Second, a virtual terminal session is established between each real application (TSO and CICS) and a virtual terminal that is associated with the multiple session manager.

Note: VTAM requires that the virtual terminal name must be different from the real terminal name.

Three VTAM sessions are established in the example in Figure 2-15:

- o Application = CA TPX Session Management for z/OS; Real Terminal = T1102015
- o Application = TSO; Virtual Terminal = TX990217
- o Application = CICS; Virtual Terminal = TX990218

Data Issues

There are several issues that must be considered when evaluating data recorded by products like NetView Session Monitor, NPM Session Subsystem, and CA NetSpy, for users accessing multiple applications through a multiple session manager.

First, data will be recorded for each real and virtual session established by the multiple session manager. In the example above, each session will be identified by session partners, as follows, where PLU is the primary logical unit, or primary session partner (usually an application), and SLU is the secondary logical unit, or secondary session partner (often a terminal).

- o CA TPX Session Management for z/OS session with real terminal

PLU = TPX
SLU = T1102015

- o Virtual terminal session with TSO

PLU = TSO
SLU = TX990217

- o Virtual terminal session with CICS

PLU = CICS
SLU = TX990218

The virtual terminals identified by SLUs TX990217 and TX990218 may bear no relationship to the real terminal, T1102015, if a multiple session manager feature called "pooling" is used. With pooling, virtual terminal names are obtained as needed from a pool of virtual terminal names. The advantage of using this feature is that new real terminals may be added to a system and their users may take advantage of a multiple session manager without requiring an update to either VTAM or tables in the host application. The disadvantage is that there is no way for an analyst or end user of the data produced for such a virtual session to determine what real terminal was in session with the host application. On the other hand, the record that contains data for the real terminal session does not identify the host application (it identifies, instead, the multiple session manager name). Where pooling is not used, data for the virtual terminal session identifies a terminal (SLU) that may be translated to the real terminal (SLU) name, but this must be understood by the analyst or user of the data in order to correctly interpret the information.

Second, network message and character counts and session connect time are included in the data for both the real terminal session and each of the virtual terminal sessions. The analyst must be careful when combining information from

these records since the results will be inflated.

Third, network response times are missing in the virtual terminal session records.

Fourth, performance monitors like Tivoli's NPM and CA NetSpy rely on the use of the definite response (DR) feature to calculate network response time. DR is an application option flag, set in the outbound message, which requires the terminal controller to return a positive indication to the application that the message arrived at the terminal. It is frequently used by host applications to synchronize transmission to the terminal. When DR is used, NPM and CA NetSpy can determine network response time as the difference between the arrival time of the DR and the time the message was sent to the terminal (with adjustments to compensate for differences in character counts between the terminal user's input message and the short message that returns as the result of a DR request).

Some multiple session managers do not pass the definite response flag on with the outbound message, but instead return an immediate DR to the host application. When this occurs, network response time is rendered meaningless.

This problem can be overcome if the network monitor provides the facility to activate DR in the VTAM interface, after the multiple session manager has already handled the outbound message. CA NetSpy is an example of a network monitor with such a feature. The CA NetSpy FORCEDR parameter is used to invoke this option.

CA NetSpy also has a multiple session manager interface that can reduce the problems these products normally present in network monitor data. This interface and its effects are described in Chapter 6.

Chapter 3: TABULAR REPORTS, GRAPHS, AND MICF INQUIRIES

Standard data displays are provided with the CA MICS Network Analyzer to help you use the data quickly and effectively. There are three categories of displays, which correspond to the display types and the method for producing them. Tabular reports consist of profile and trend formats and provide hard copy numeric data displays. Sample graphics are basic color graphics reports distributed as samples and are meant to be used as the basis for developing tailored reports at each installation. MICF inquiries are precomposed printer reports and color graphics which are invoked using the CA MICS Information Center Facility (MICF).

This section contains the following topics:

[3.1 Tabular Reports](#) (see page 162)

[3.2 Sample Graphics](#) (see page 283)

[3.3 MICF Inquiries](#) (see page 304)

3.1 Tabular Reports

Standard tabular reports provide hardcopy numeric displays of data on a regular basis.

There are two classifications of tabular reports -- profile and trend.

PROFILES

Profile reports present data as groups of individual summary values (averages, minimums, maximums, etc.) over a given period of time (day, week, month, etc.). Profile reports give a snapshot of a specific area of operation during that time and are employed when a specific value of a measured element indicates a desirable or undesirable condition. Thus, profiles are used in conjunction with a set of threshold values which may be either implicitly understood or explicitly stated on the report.

TRENDS

Trend reports present data as a series of measured values displayed together to show the nature of the change of a condition over a period of time. They are used when the rate of change of a measure or the exact time at which a given measured value was reached is more important than the actual measure of the value itself.

Trend reports display the values of key data elements specific to a given activity area for three sequential time intervals (e.g., the last three months). To find the change in the measured values over a time period, the size, rate, and percentage of change are calculated.

The key to applying a profile or trend report is understanding the usage considerations for which it was developed. Usage considerations for this Analyzer are discussed in Chapter 2.

Instructions for producing the reports, report descriptions, and sample report formats are discussed in the following sections:

- 1 - Producing Tabular Reports
- 2 - Tabular Report Formats
- 3 - Tabular Report Descriptions

3.1.1 Producing Tabular Reports

The CA MICS Network Analyzer's standard tabular reports are produced by a report generator routine. That is, no fixed format routine exists to produce each specific report format. Rather, a set of routines, including data selection, data sequencing, summarization, and display, are custom-generated based on your parameter specifications.

The network report generator is invoked by executing the MICSSHRx procedure and using the SAS %INCLUDE function to include sharedprefix.MICS.INCLLIB(SNTRPTS). This member, in turn, includes the required macro sets, prepares the environment, and brings in the report generator code.

You may produce these reports for any timespan in which the data exists. To facilitate your production of reports in the most frequently used timespans, two sample jobs are generated during installation and are saved in prefix.MICS.PARMS as members SNTRPTD and SNTRPTM. The first executes each of the reports from the DAYS timespan; the second invokes each report using the MONTHS timespan.

If you wish, you may provide your own job to invoke the reports. Sample JCL to produce the daily reports follows:

```
//jobname JOB (acct fields), . . . .
//REPORTS EXEC MICSSHRx
//INPUTRPT DD DSN=prefix.MICS.PARMS(SNTRPTD),DISP=SHR
//SYSIN DD *
           %INCLUDE INCLLIB(SNTRPTS);
/*
```

To run the monthly reports, substitute member SNTRPTM for SNTRPTD in prefix.MICS.PARMS in the INPUTRPT DD statement above.

Keep in mind that, depending on such things as the size of your network, the number of applications, and the number of terminal sessions represented in your network monitor data, the output from running either of these sample jobs can be substantial. One way to reduce the quantity of output is to code a data selection macro, as described in Section 3.1.1.2, to subset your data for reporting purposes.

The report generator can produce several reports, many in multiple formats. You may select data for a given report from any timespan in which the requisite file is supported. That data can be further subset to specific areas of

interest. This flexibility is controlled by a combination of report generator control statements and user-coded SAS macros, which are discussed in the following sections:

- 1 - Report Selection
- 2 - Report Customizing
- 3 - Integrating Reports into the DAILY CA MICS Job

3.1.1.1 Report Selection

The report generator reads a parameter list from the DD statement named INPUTRPT. This parameter list indicates the reports that have been chosen, the format in which they are to be produced, the timespan from which data for the reports is to be extracted, and the desired cycles of the timespan. The rules for coding these parameters are explained below.

A report generator's input parameter list consists of one or more report statements in the following format:

REPORT SNTnnn format timespan cycle

where:

REPORT Keyword with which each report selection statement must begin. A report is produced from each correctly coded statement. Lines beginning with asterisks (*) are considered comments. Blank lines are ignored; you may use them to format your report.

SNTnnn Six-character identifier that consists of the characters, SNT, followed by a three-digit number. Valid report identifiers are the following:

SNT101	NPM Service by Application
SNT103	NPM Service by Link
* SNT105	NLDM Service by Performance Class
SNT111	NLDM Service by Application
SNT112	NLDM Service by Link
SNT113	NLDM Service by Control Unit
SNT114	NLDM Service by Terminal
* SNT115	NLDM Service by Performance Class
SNT121	NetSpy Service by Application
SNT122	NetSpy Service by Terminal
SNT201	NPM Workload by Application
SNT203	NPM Workload by Link
SNT208	NPM/NetSpy Utilization by NCP
SNT209	NPM/NetSpy NCP Utilization by Link
SNT211	NLDM Workload by Application
SNT212	NLDM Workload by Link
SNT213	NLDM Workload by Control Unit
SNT214	NLDM Workload by Terminal
SNT215	NPM/NetSpy NCP Utilization by Link
SNT216	NPM/NetSpy NCP Utilization by Link
SNT221	NetSpy Workload by Application

SNT222	NetSpy Workload by Terminal
SNT401	NPM/NetSpy NCP Link Data Collection
SNT403	NPM Session Data Collection
SNT601	NPDA Event Analysis
SNT602	NPDA Statistics Analysis

* SNT105 is derived from the SNTNSV file, while
SNT115 is derived from the NVSRTM file.

format Indicates the format of the report produced:
PROFILE or TREND. Profile reports display
information derived from a single cycle of data
while trend reports display information from
multiple cycles.

timespan Indicates the database timespan that contains the
data for the report. The timespan field contains
a single-character indicator. The possible
choices follow:

X	DETAIL Timespan
D	DAYS Timespan
W	WEEKS Timespan
M	MONTHS Timespan
Y	YEARS Timespan

Note: The file used for the report must exist in
the requested timespan for a report to be
produced. The files used by each report are
listed in Figure 3-2, CA MICS Network Analyzer
Tabular Reports List.

cycle Defines the database cycle that is used for the
report when the profile format is requested. When
the trend format is requested, cycle defines the
first of three consecutive cycles.

Note: All three cycles do not have to be
present for trend reports, but certain fields
on the report will be blank if the data is not
available.

You can specify as many report statements as you need in any
order.

Examples:

```
REPORT SNT101 PROFILE D 01  
REPORT SNT101 TREND D 01
```

REPORT SNT103 PROFILE D 01
REPORT SNT103 TREND D 01

3.1.1.2 Report Customizing

Because of the potentially large volume of data made available by the CA MICS Network Analyzer, any one of the standard reports may produce an inordinately large output, much of which may be of little interest. To limit this output, provisions have been made to allow you to select the data explicitly. This is accomplished through the use of user-coded selection macros written in the SAS language.

There is one data selection macro for each of the standard report types generated by the CA MICS report generator. These macros have names starting with '%SL', followed by a three-digit Report-ID number. Thus, the data selection macro for the SNT101 report is: %SL101.

The data selection macro stubs reside in sharedprefix.MICS.SOURCE(#SNTRPTS). Copy the macro stub to prefix.MICS.USER.SOURCE(#SNTRPTS) after the %INCLUDE for SOURCE(#SNTRPTS) and add any selection criteria. The macros are invoked in a SAS DATA step prior to any sorting or summarization for reporting. Thus, any SAS statement which is valid in a DATA step may be coded in these macros.

IMPORTANT: Only simple selection statements are permitted within the macros since the data is in a predetermined order that you cannot modify. Therefore, using FIRST. or LAST. coding and similar data-sequence-dependent functions within the macros will not work.

A set of null macros is supplied with the Analyzer and will be concatenated ahead of prefix.MICS.USER.SOURCE(#SNTRPTS) in the input stream. This prevents a SAS 180 error from occurring in case you delete and do not replace one of the sample macros from prefix.MICS.USER.SOURCE.

In the following example, the NLDM Service by Performance Class Report is to be produced only for the critical performance class, TSODEV, TSO Development. The selection logic in the %SL105 report is as follows. Figure 3-2 lists each report and its corresponding report ID. The arrows (==>) in this example indicate user-developed code.

```
/* SNT105 REPORT OBSERVATION SELECTION MACRO */
==> /* SELECT ONLY PERFORMANCE CLASS 'TSODEV' */
%MACRO SL105;
==> IF NSVPCLSS = 'TSODEV';
%MEND SL105;
```


3.1.1.3 Integrating Reports into the DAILY Job

CA MICS Network Analyzer tabular reports can be incorporated into the CA MICS DAILY update job stream in the DAY500 step. Listed below are the implementation guidelines. You should follow all the steps in the order given.

- 1 - In prefix.MICS.USER.SOURCE(DYUSER), code the following SAS statement.

```
%INCLUDE INCLLIB(SNTRPTS);
```

- 2 - Using IEBUPDTE, add the INPUTRPT DD statement (as described in Section 3.1.1) to sharedprefix.MICS.PROTOLIB(DYUSR500) after the existing SYSIN DD statement. Since you may not wish to make this change for all units in the complex, you can include the generator control language below in the IEBUPDTE to check for the prefix of the unit database being processed.

```
:IF &PREFIX NE &STR(uprefix) THEN GOTO c
//INPUTRPT DD DSN=prefix.MICS.PARMS(SNTRPTS),DISP=SHR
:c:
```

In the above example, 'uprefix' is your unit database prefix and 'c' is a label which you define. For more information on the generator control language, refer to Section 2.3.3.3.3 of the CA MICS PIOM Guide.

Also, the prefix.MICS.PARMS(SNTRPTS) member would contain the report selection parameters for the specific reports you want to produce every day. You should code these report selection parameters according to the format described in Section 3.1.1.1 of this guide.

- 3 - In prefix.MICS.PARMS(JCLGENU), code the word DAILY, and then submit prefix.MICS.CNTL(JCLGENU). This step regenerates your DAILY operational job stream.

Make changes to the DAILY or any other CA MICS job in sharedprefix.MICS.PROTOLIB so that they will not be overridden in future regenerations.

3.1.2 Tabular Report Formats

The tabular reports present the values of key data elements as formatted rectangular arrays of numbers.

There are three major areas on each tabular report:

- o Report Heading
- o Data Element Descriptions
- o Data Area

The relative positions of each of these areas is shown in the following diagram.

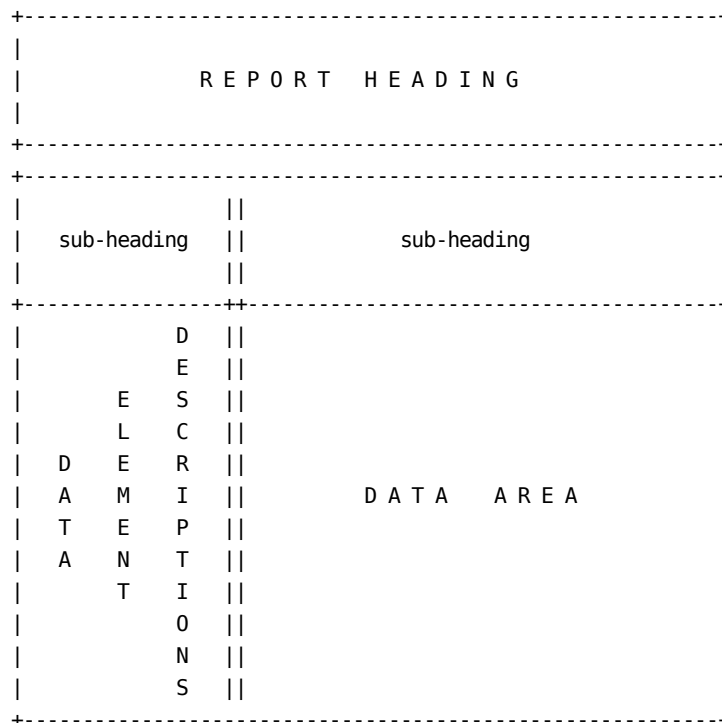


Figure 3-1. Tabular Report Format

Each of the tabular reports can be produced in one of two formats: profile or trend. Both formats of a given report present the same data elements, in the same relative positions on the page, but for different time-period summaries of the data.

3.1.3 Tabular Report Descriptions

Separate classes of tabular reports are defined for the CA MICS Network Analyzer. Within each class are one or more specific reports, each presenting data from one file. Figure 3-2 shows the various reports, their classes, and the files from which they are produced.

Note that any tabular report beginning with the name of the data source NetView NLDM can also be produced from equivalent data collected by CA NetMaster NTS. Any report beginning with the name of the data source NetView NPDA can also be produced from equivalent data collected by CA NetMaster NEWS.

Placeholders have been left in this chapter to add reports in three additional report classes. The information currently processed by CA MICS does not support these reports.

Each report of a given class displays similar types of data, but the individual data elements are tailored to the file from which the data is obtained and limited by the data source from which it was originally derived. Thus, a service report produced from NPM data displays host, network, and total response time, while an NLDM service report shows only total response time.

The content of each report is discussed in greater detail in the following sections:

- 1 - Service Analysis Reports
- 2 - Workload Analysis Reports
- 3 - CA MICS Class 3 Reports
(this class is not currently supported)
- 4 - Data Collection Reports
- 5 - CA MICS Class 5 Reports
(this class is not currently supported)
- 6 - Network Incident Reports
- 7 - CA MICS Class 7 Reports
(this class is not currently supported)

NETWORK ANALYZER					
Tabular Reports List					
Report Class	Report Name	Report ID	Data Base File	Sample Figure No.	
				Profile	Trend
Service Analysis Reports	NPM Service by Application	SNT101	SNTPSY	3-3	3-3A
	NPM Service by Link	SNT103	SNTNPL	3-4	3-4A
	*NLDM Service by Performance Class	SNT105	SNTNSV	3-5	3-5A
	*NLDM Service by Application	SNT111	NVLSY	3-6	
	*NLDM Service by Link	SNT112	NVSNLL	3-7	
	*NLDM Service by Control Unit	SNT113	NVSRM	3-8	
	*NLDM Service by Terminal	SNT114	NVSRM	3-9	
	*NLDM Service by Performance Class	SNT115	NVSRM	3-10	
	NetSpy Service by Application	SNT121	SNTNSP	3-11	
	NetSpy Service by Terminal	SNT122	SNTNSS	3-12 =>	3-12C
Workload Analysis Reports	NPM Workload by Application	SNT201	SNTPSY	3-13	3-13A
	NPM Workload by Link	SNT203	SNTNPL	3-14	3-14A
	NPM Utilization by NCP	SNT208	SNTNAF	3-15	3-15A
	NetSpy Utilization by NCP	SNT208	SNTNAF	3-16	3-16A
	NPM NCP Utilization by Link	SNT209	SNTNCL	3-17 =>	3-17C
	NetSpy NCP Utilization by Link	SNT209	SNTNCL	3-18	3-18A
	*NLDM Workload by Application	SNT211	NVLSY	3-19	
	*NLDM Workload by Link	SNT212	NVSNLL	3-20	
	*NLDM Workload by Control Unit	SNT213	NVNSA	3-21	
	*NLDM Workload by Terminal	SNT214	NVNSA	3-22	
	NPM NCP Utilization by Link	SNT215	SNTNCL	3-23 =>	3-23E
	NetSpy NCP Utilization by Link	SNT215	SNTNCL	3-24 =>	3-24C
	NPM NCP Utilization by Link	SNT216	SNTNCL	3-25	
	NetSpy NCP Utilization by Link	SNT216	SNTNCL	3-26	
	NetSpy Workload by Application	SNT221	SNTNSP	3-27	
	NetSpy Workload by Terminal	SNT222	SNTNSS	3-28 =>	3-28C
Data Collection Reports	NPM NCP Link Data Collection	SNT401	SNTNCL	3-29	3-29A
	NetSpy NCP Link Data Collection	SNT401	SNTNCL	3-30	
	NPM Session Data Collection	SNT403	SNTNPL	3-31	3-31A
Incident Analysis Reports	*NPDA Event Analysis	SNT601	SNTNEF	3-32	3-32A
	*NPDA Statistics Analysis	SNT602	SNTNSF	3-33	3-33A

*Any report beginning with NLDM can also be produced from equivalent data collected by CA NetMaster NTS product, and any report beginning with NPDA can also be produced from equivalent data collected by CA NetMaster NEWS product.

Figure 3-2. CA MICS Network Analyzer Tabular Reports List

3.1.3.1 Service Analysis Reports

Service analysis reports indicate the service level provided by the network to a given group of users. You can produce these reports either in profile format or in trend format. Profile reports display data that is retained in a single cycle of the CA MICS database. Trend reports compare three cycles of data.

Any report in the sections listed below with the name of the data source NLDM can also be produced from equivalent data collected by the CA NetMaster NTS product.

The service analysis reports are explained in greater detail in the following sections:

- 1 - NPM Service by Application (SNT101)
- 2 - NPM Service by Link (SNT103)
- 3 - NLDM Service by Performance Class (SNT105) *
- 4 - NLDM Service by Application (SNT111)
- 5 - NLDM Service by Link (SNT112)
- 6 - NLDM Service by Control Unit (SNT113)
- 7 - NLDM Service by Terminal (SNT114)
- 8 - NLDM Service by Performance Class (SNT115) *
- 9 - NetSpy Service by Application (SNT121)
- 10 - NetSpy Service by Terminal (SNT122)

* The SNT105 Report is derived from the SNTNSV file
while the SNT115 Report is derived from the NVSRTM file.

3.1.3.1.1 NPM Service by Application (SNT101)

INTENDED USAGE:

This report shows the total level of service experienced by users of the specified host application or primary logical unit (PLU). Where possible, the separate network and host components of the total service are also shown. This report is useful in determining whether a response time problem experienced by users of an application results from delays in the host or in the network. This report can also help you to determine how widespread a response time problem is by comparing the response times and response time components for separate applications.

FORMAT:

This display indicates the average and maximum host, network, and total response times for selected applications. In addition the host, network, and total response distributions are given. Sample displays of profile and trend reports are shown in Figures 3-3 and 3-3A.

DATABASE FILE: SNTPSY

DATA ELEMENTS USED:

NPMLOHST	NPMHIHST	NPMLONET	NPMHINET	NPMLTOT	NPMHITOT
NPMRVAL1	NPMRVAL2	NPMRVAL3	NPMRVAL4		
PSYAVHTM	PSYMXHTM	PSYHRESC	PSYNRHRE	PSYAVNTM	PSYMXNTM
PSYNRESC	PSYNRNRE	PSYAVTTM	PSYPCTR1	PSYPCTR2	PSYPCTR3
PSYPCTR4	PSYMXTTM	PSYTRESC	PSYNRTRE	PLU	

CALCULATIONS:

Percent of Responses without Network Response =

$$((\text{PSYTRESC} - \text{PSYNRESC}) / \text{PSYTRESC}) * 100;$$

USAGE CONSIDERATIONS:

You can vary the specific PLUs for which reports are produced by changing the value of the %SL101 macro in the member prefix.MICS.USER.SOURCE(#SNTRPTS). The default macro in prefix.MICS.USER.SOURCE(#SNTRPTS) selects all PLUs.

In some cases you may find that network service values are missing or zero. This is because NPM only collects network response times if Definite Response (DR) is requested when the terminal output operation is requested. In a CICS system, DR may be optionally requested for each CICS transaction. The last line on the report, PCT RESPONSES WITH NO NET RESP, provides the percentage of responses for which DR was not active. If this value is 100%, then you should expect the network service values to be zero since this indicates that DR has not been requested for any of the transactions. Values approaching 100% are an indication that the reported network service values are only representing a small percentage of the total number of transactions and may not be indicative of the actual service experienced by all users of the application.

CA MICS NETWORK COMPONENT

(SNT101) NPM SERVICE BY APPLICATION: CICSPROD

NETWORK: NETWORK1 SYSTEM: 3084
 PRODUCED: OCTOBER 20, 2003 ZONE: PRIME TIME

+-----+	
ACTIVITY INDICATORS	10/18/03
+-----+	
HOST SERVICE	
AVERAGE HOST RESPONSE TIME	0:00.51
MAXIMUM HOST RESPONSE TIME	0:12.19
NO. OF HOST RESPONSES	1,494
HOST RESPONSES NOT IN RANGE	
0 - 1 SECS	178
NETWORK SERVICE	
AVERAGE NETWORK RESPONSE TIME	0:01.47
MAXIMUM NETWORK RESPONSE TIME	0:06.13
NO. OF NETWORK RESPONSES	1,437
NETWRK RESPONSES NOT IN RANGE	
0 - 0 SECS	6
TOTAL SERVICE	
AVERAGE TOTAL RESPONSE TIME	0:01.97
PERCENT WITHIN 1 SECS	14.26
PERCENT WITHIN 2 SECS	59.37
PERCENT WITHIN 3 SECS	88.02
PERCENT WITHIN 5 SECS	97.79
MAXIMUM TOTAL RESPONSE TIME	0:13.37
TOTAL NO. OF RESPONSES	1,494
TOTAL RESPONSES NOT IN RANGE	
0 - 0 SECS	2
PCT RESPONSES WITH NO NET RESP	3.82
+-----+	

Figure 3-3. NPM Service by Application (Profile)

CA MICS NETWORK COMPONENT						
(SNT101) NPM SERVICE BY APPLICATION: CICSPROD						
NETWORK: NETWORK1 SYSTEM: 3084						
PRODUCED: OCTOBER 20, 2003 ZONE: PRIME TIME						
ACTIVITY INDICATORS	10/18/03	10/17/03	10/16/03	AMOUNT OF CHANGE SINCE 10/16/03	PER-PERIOD RATE OF CHANGE SINCE 10/16/03	PERCENTAGE CHANGE SINCE 10/16/03
HOST SERVICE						
AVERAGE HOST RESPONSE TIME	0:00.51	0:00.66	0:00.66	-0:00.15	-0.08	-22.93
MAXIMUM HOST RESPONSE TIME	0:12.19	0:07.02	0:05.83	0:06.36	3.18	109.09
NO. OF HOST RESPONSES	1,494	1,622	1,228	266	133.00	21.66
HOST RESPONSES NOT IN RANGE 0 - 1 SECS	178	316	252	-74	-37.00	-29.37
NETWORK SERVICE						
AVERAGE NETWORK RESPONSE TIME	0:01.47	0:01.61	0:01.56	-0:00.09	-0.05	-6.08
MAXIMUM NETWORK RESPONSE TIME	0:06.13	0:08.76	0:05.38	0:00.75	0.38	13.94
NO. OF NETWORK RESPONSES	1,437	1,573	1,198	239	119.50	19.95
NETWRK RESPONSES NOT IN RANGE 0 - 4 SECS	6	33	9	-3	-1.50	-33.33
TOTAL SERVICE						
AVERAGE TOTAL RESPONSE TIME	0:01.97	0:02.25	0:02.20	-0:00.23	-0.11	-10.40
PERCENT WITHIN 1 SECS	14.26	11.96	9.20	5.05	2.53	54.93
PERCENT WITHIN 2 SECS	59.37	52.09	53.18	6.19	3.10	11.64
PERCENT WITHIN 3 SECS	88.02	77.19	79.48	8.54	4.27	10.74
PERCENT WITHIN 4 SECS	97.79	90.93	93.48	4.30	2.15	4.60
MAXIMUM TOTAL RESPONSE TIME	0:13.37	0:08.89	0:07.90	0:05.47	2.74	69.24
TOTAL NO. OF RESPONSES	1,494	1,622	1,228	266	133.00	21.66
TOTAL RESPONSES NOT IN RANGE 0 - 6 SECS	2	23	6	-4	-2.00	-66.67
PCT RESPONSES WITH NO NET RESP	3.82	3.02	2.44	1.37	0.69	56.17

Figure 3-3A. NPM Service by Application (Trend)

3.1.3.1.2 NPM Service by Link (SNT103)

INTENDED USAGE:

This display quantifies the service provided by the network to the users of a given boundary link. This display is used to determine if a network performance problem is isolated to a given link.

FORMAT:

This display indicates the average and maximum host, network, and total response times for selected links. It also gives the host, network, and total response distributions. You can see sample displays of profile and trend reports in Figures 3-4 and 3-4A.

DATABASE FILE: SNTNPL

DATA ELEMENTS USED:

SLULINK	ZONE				
NPMLOHST	NPMHIHST	NPMLONET	NPMHINET	NPMLOTOT	NPMHITOT
NPMRVAL1	NPMRVAL2	NPMRVAL3	NPMRVAL4		
NPLAVHTM	NPLMXHTM	NPLHRESC	NPLNRHRE	NPLAVNTM	NPLMXNTM
NPLNRESC	NPLNRNRE	NPLAVTTM	NPLPCTR1	NPLPCTR2	NPLPCTR3
NPLPCTR4	NPLMXTTM	NPLTRESC	NPLNRTRE		

CALCULATIONS:

Pct Responses with No Net Resp =

$$((NPLTRESC - NPLNRESC)/NPLTRESC) * 100;$$

USAGE CONSIDERATIONS:

You can vary the number of links for which reports are produced by changing the value of the %SL103 macro in prefix.MICS.USER.SOURCE(#SNT103). The default macro selects all links.

CA MICS NETWORK COMPONENT		
(SNT103) NPM SERVICE BY LINK: SFLINK1		
NETWORK: NETWORK1 SYSTEM: 3084		
PRODUCED: OCTOBER 20, 2003 ZONE: PRIME TIME		
+-----+		
ACTIVITY INDICATORS	10/17/03	
+-----+		
HOST SERVICE		
AVERAGE HOST RESPONSE TIME	0:00.51	
MAXIMUM HOST RESPONSE TIME	0:12.19	
NO. OF HOST RESPONSES	1,494	
HOST RESPONSES NOT IN RANGE		
0 - 1 SECS	178	
NETWORK SERVICE		
AVERAGE NETWORK RESPONSE TIME	0:01.47	
MAXIMUM NETWORK RESPONSE TIME	0:06.13	
NO. OF NETWORK RESPONSES	1,437	
NETWRK RESPONSES NOT IN RANGE		
0 - 4 SECS	6	
TOTAL SERVICE		
AVERAGE TOTAL RESPONSE TIME	0:01.97	
PERCENT WITHIN 1 SECS	14.26	
PERCENT WITHIN 2 SECS	59.37	
PERCENT WITHIN 3 SECS	88.02	
PERCENT WITHIN 4 SECS	97.79	
MAXIMUM TOTAL RESPONSE TIME	0:13.37	
TOTAL NO. OF RESPONSES	1,494	
TOTAL RESPONSES NOT IN RANGE		
0 - 6 SECS	2	
PCT RESPONSES WITH NO NET RESP	3.82	
+-----+		

Figure 3-4. NPM Service by Link (Profile)

CA MICS NETWORK COMPONENT						
(SNT103) NPM SERVICE BY LINK: SFLINK1						
NETWORK: NETWORK1 SYSTEM: 3084						
PRODUCED: OCTOBER 20, 2003 ZONE: PRIME TIME						
ACTIVITY INDICATORS	10/17/03	10/16/03	10/15/03	AMOUNT OF CHANGE SINCE 10/15/03	PER-PERIOD RATE OF CHANGE SINCE 10/15/03	PERCENTAGE CHANGE SINCE 10/15/03
HOST SERVICE						
AVERAGE HOST RESPONSE TIME	0:00.51	0:00.66	0:00.66	-0:00.15	-0.08	-22.93
MAXIMUM HOST RESPONSE TIME	0:12.19	0:07.02	0:05.83	0:06.36	3.18	109.09
NO. OF HOST RESPONSES	1,494	1,622	1,228	266	133.00	21.66
HOST RESPONSES NOT IN RANGE 0 - 1 SECS	178	316	252	-74	-37.00	-29.37
NETWORK SERVICE						
AVERAGE NETWORK RESPONSE TIME	0:01.47	0:01.61	0:01.56	-0:00.09	-0.05	-6.08
MAXIMUM NETWORK RESPONSE TIME	0:06.13	0:08.76	0:05.38	0:00.75	0.38	13.94
NO. OF NETWORK RESPONSES	1,437	1,573	1,198	239	119.50	19.95
NETWRK RESPONSES NOT IN RANGE 0 - 4 SECS	6	33	9	-3	-1.50	-33.33
TOTAL SERVICE						
AVERAGE TOTAL RESPONSE TIME	0:01.97	0:02.25	0:02.20	-0:00.23	-0.11	-10.40
PERCENT WITHIN 1 SECS	14.26	11.96	9.20	5.05	2.53	54.93
PERCENT WITHIN 2 SECS	59.37	52.09	53.18	6.19	3.10	11.64
PERCENT WITHIN 3 SECS	88.02	77.19	79.48	8.54	4.27	10.74
PERCENT WITHIN 4 SECS	97.79	90.93	93.48	4.30	2.15	4.60
MAXIMUM TOTAL RESPONSE TIME	0:13.37	0:08.89	0:07.90	0:05.47	2.74	69.24
TOTAL NO. OF RESPONSES	1,494	1,622	1,228	266	133.00	21.66
TOTAL RESPONSES NOT IN RANGE 0 - 6 SECS	2	23	6	-4	-2.00	-66.67
PCT RESPONSES WITH NO NET RESP	3.82	3.02	2.44	1.37	0.69	56.17

Figure 3-4A. NPM Service by Link (Trend)

3.1.3.1.3 NLDM Service by Performance Class (SNT105)

INTENDED USAGE:

Use this display to quantify the service level provided by the network to a given user group identified by the NLDM Performance Class (NSVPCCLSS). If the NLDM performance classes conform to the classification specified in the site's service level agreements, this display will be useful in tracking the site's adherence to its commitments.

FORMAT:

This display shows the average total response time and the total response time distributions for the selected performance class. In addition, the display shows the the percentage of all transactions and the percentage of individual collection intervals that met the RTM response time objective for the selected performance class. You can see sample displays of profile and trend reports in figures 3-5 and 3-5A.

DATABASE FILE: SNTNSV

DATA ELEMENTS USED:

NSVPCCLSS	ZONE	NLDRVAL1	NLDRVAL2	NLDRVAL3	NLDRVAL4
NSVAVTTM	NSVPCTR1	NSVPCTR2	NSVPCTR3	NSVPCTR4	NSVTRESC

CALCULATIONS:

None

USAGE CONSIDERATIONS:

You can report on different performance classes by changing the value of the %SL105 macro in prefix.MICS.USER.SOURCE(#SNTRPTS). The default macro selects all performance classes.

CA MICS NETWORK COMPONENT

(SNT105) NLDM SERVICE BY PERFORMANCE CLASS: TSOPROD

NETWORK: NETWORK1 SYSTEM: 3084

PRODUCED: OCTOBER 20, 2003 ZONE: PRIME TIME

ACTIVITY INDICATORS		10/16/03
TOTAL SERVICE		
OBJECTIVE	90% < 3	
% MET OVERALL		89.34
% MET BY SAMPLED INTERVALS		35.90
AVERAGE TOTAL RESPONSE TIME		0:01.95
% OF TOTAL RESPONSES < 1 SEC		47.42
% OF TOTAL RESPONSES < 3 SEC		89.34
% OF TOTAL RESPONSES < 5 SEC		95.69
% OF TOTAL RESPONSES < 10 SEC		98.33
TOTAL NO. OF RESPONSE EVENTS		21,682
TOTAL NO. OF SAMPLED INTERVALS		390

Figure 3-5. NLDM Service by Performance Class (Profile)

CA MICS NETWORK COMPONENT						
(SNT105) NLDM SERVICE BY PERFORMANCE CLASS: TSOPROD						
NETWORK: NETWORK1 SYSTEM: 3084						
PRODUCED: OCTOBER 20, 2003 ZONE: PRIME TIME						
ACTIVITY INDICATORS	10/16/03	10/15/03	10/14/03	AMOUNT OF CHANGE SINCE 10/14/03	PER-PERIOD RATE OF CHANGE SINCE 10/14/03	PERCENTAGE CHANGE SINCE 10/14/03
TOTAL SERVICE						
OBJECTIVE 90% < 3						
% MET OVERALL	89.34	89.63	89.34	0.00	0.00	0.00
% MET BY SAMPLED INTERVALS	35.90	36.39	35.90	0.00	0.00	0.00
AVERAGE TOTAL RESPONSE TIME	0:01.95	0:01.90	0:01.95	0:00.00	0.00	0.00
% OF TOTAL RESPONSES < 1 SEC	47.42	48.92	47.42	0.00	0.00	0.00
% OF TOTAL RESPONSES < 3 SEC	89.34	89.63	89.34	0.00	0.00	0.00
% OF TOTAL RESPONSES < 5 SEC	95.69	95.79	95.69	0.00	0.00	0.00
% OF TOTAL RESPONSES < 10 SEC	98.33	98.36	98.33	0.00	0.00	0.00
TOTAL NO. OF RESPONSE EVENTS	21,682	22,601	21,682	0	0.00	0.00
TOTAL NO. OF SAMPLED INTERVALS	390	393	390	0	0.00	0.00

Figure 3-5A. NLDM Service by Performance Class (Trend)

3.1.3.1.4 NLDM Service by Application (SNT111)

INTENDED USAGE:

Use this display to quantify the service level the network provides to a given primary logical unit (PLU). Use this display for tracking the site's performance for applications.

FORMAT:

This display indicates the average total response times for the selected applications and gives response distributions. Figure 3-6 is a sample display of the profile report.

DATABASE FILE: NVLSY

DATA ELEMENTS USED:

PLU	ZONE	NLDRVAL1	NLDRVAL2	NLDRVAL3	NLDRVAL4
LSYPCOBM	LSYAVTTM	LSYPCTR1	LSYPCTR2	LSYPCTR3	LSYPCTR4
LSYTRESC					

CALCULATIONS:

None

USAGE CONSIDERATIONS:

You can report on different PLUs by changing the value of the %SL111 macro in prefix.MICS.USER.SOURCE(#SNTRPTS). The default macro selects all PLUs.

CA MICS NETWORK COMPONENT

(SNT111) NLDM SERVICE BY APPLICATION: CICSACPB

NETWORK: NETWORK1 SYSTEM: TS01

PRODUCED: AUGUST 7, 2003 ZONE: PRIME TIME

ACTIVITY INDICATORS	08/04/03
TOTAL SERVICE	
RESPONSE COUNT	512
RESPONSE TIME	0:13:56.70
AVERAGE RESPONSE TIME	0:01.63
CUMULATIVE RESPONSE PERCENT	
WITHIN 1.0 SECS	24.02
WITHIN 3.0 SECS	94.73
WITHIN 5.0 SECS	99.22
WITHIN 10.0 SECS	100.00
RESPONSE DISTRIBUTION COUNT	
UNDER 1.0 SECS	123
BETWEEN 1.0 - 3.0 SECS	362
BETWEEN 3.0 - 5.0 SECS	23
BETWEEN 5.0 - 10.0 SECS	4
OVER 10.0 SECS	0

Figure 3-6. NLDM Service by Application (Profile)

3.1.3.1.5 NLDM Service by Link (SNT112)

INTENDED USAGE:

Use this display to quantify the service level the network provides to a given link (SLULINK). Use this display for tracking your site's performance for links.

FORMAT:

This display indicates the average total response times for the selected link and gives response distributions. You can see a sample display of the profile report in Figure 3-7.

DATABASE FILE: NVSNLL

DATA ELEMENTS USED:

SLULINK	ZONE	NLDRVAL1	NLDRVAL2	NLDRVAL3	NLDRVAL4
NLLPCOBM	NLLAVTTM	NLLPCTR1	NLLPCTR2	NLLPCTR3	NLLPCTR4
NLLTRES					

CALCULATIONS:

None

USAGE CONSIDERATIONS:

You can report on different SLULINKs by changing the value of the %SL112 macro in prefix.MICS.USER.SOURCE(#SNT112). The default macro selects all SLULINKs.

CA MICS NETWORK COMPONENT		
(SNT112) NLDM SERVICE BY LINK: L1000		
NETWORK: NETWORK1 SYSTEM: TS02		
PRODUCED: AUGUST 7, 2003 ZONE: GRAVE		
+-----+		
ACTIVITY INDICATORS	08/04/03	
+-----+		
TOTAL SERVICE		
AVERAGE TOTAL RESPONSE TIME	0:03.30	
CUMULATIVE RESPONSE PERCENT		
WITHIN 1.0 SECS	47.37	
WITHIN 5.0 SECS	100.00	
WITHIN 7.0 SECS	100.00	
WITHIN 10.0 SECS	100.00	
TOTAL NO. OF RESPONSE EVENTS	19	
+-----+		

Figure 3-7. NLDM Service by Link (Profile)

3.1.3.1.6 NLDM Service by Control Unit (SNT113)

INTENDED USAGE:

Use this display to quantify the service level the network provides to a given control unit (SLUPU). Use this display for tracking your site's performance for control units.

The job that produces this display will not execute or will cause unpredictable results unless both the value and the label for account code SNTACT3 is set to SLUPU for NetView/NLDM or CA NetMaster data. For information on how to define account codes, refer to Section 7.2.

FORMAT:

This display indicates the average total response times for the selected control unit and gives response distributions. A sample display of the profile report is shown in Figure 3-8.

DATABASE FILE: NVSRTM

DATA ELEMENTS USED:

SLUPU	ZONE	NLDRVAL1	NLDRVAL2	NLDRVAL3	NLDRVAL4
RTMPCOBM	RTMAVTTM	RTMPCTR1	RTMPCTR2	RTMPCTR3	RTMPCTR4
RTMTRESC					

CALCULATIONS:

None

USAGE CONSIDERATIONS:

You can report on different SLUPUs by changing the value of the %SL113 macro in prefix.MICS.USER.SOURCE(#SNT113). The default macro selects all SLUPUs.

CA MICS NETWORK COMPONENT
 (SNT113) NLDM SERVICE BY CONTROL UNIT (SLUPU): R13CU1

NETWORK: NETWORK1 SYSTEM: TS01
 PRODUCED: AUGUST 7, 2003 ZONE: PRIME TIME

+-----+	
ACTIVITY INDICATORS	08/04/03
+-----+	
TOTAL SERVICE	
OBJECTIVE 90.0 < 3.0	
% MET OVERALL	93.57
% MET BY SAMPLED INTERVALS	57.14
AVERAGE TOTAL RESPONSE TIME	0:01.63
TOTAL NO. OF RESPONSE EVENTS	716
TOTAL NO. OF SAMPLED INTERVALS	21
CUMULATIVE RESPONSE PERCENT	
WITHIN 1.0 SECS	28.49
WITHIN 3.0 SECS	93.57
WITHIN 5.0 SECS	98.74
WITHIN 10.0 SECS	99.86
RESPONSE DISTRIBUTION COUNT	
UNDER 1.0 SECS	204
BETWEEN 1.0 - 3.0 SECS	466
BETWEEN 3.0 - 5.0 SECS	37
BETWEEN 5.0 - 10.0 SECS	8
OVER 10.0 SECS	1
+-----+	

Figure 3-8. NLDM Service by Control Unit (Profile)

3.1.3.1.7 NLDM Service by Terminal (SNT114)

INTENDED USAGE:

Use this display to quantify the service level the network provides to a given terminal (SLU). Use this display for tracking your site's performance for terminals.

FORMAT:

This display indicates the average total response times for the selected terminal and gives response distributions. A sample display of the profile report is shown in Figure 3-9.

DATABASE FILE: NVSRTM

DATA ELEMENTS USED:

SLU	ZONE	NLDRVAL1	NLDRVAL2	NLDRVAL3	NLDRVAL4
RTMPCOBM	RTMAVTTM	RTMPCTR1	RTMPCTR2	RTMPCTR3	RTMPCTR4
RTMTRESC					

CALCULATIONS:

None

USAGE CONSIDERATIONS:

You can report on different SLUs by changing the value of the %SL114 macro in prefix.MICS.USER.SOURCE(#SNTRPTS). The default macro selects all SLUs.

CA MICS NETWORK COMPONENT

(SNT114) NLDM SERVICE BY TERMINAL (SLU): R329

NETWORK: NETWORK1 SYSTEM: TS01

PRODUCED: AUGUST 7, 2003 HOUR: 11

ACTIVITY INDICATORS	08/04/03
TOTAL SERVICE	
OBJECTIVE 90.0% < 3.0	
% MET OVERALL	95.40
% MET BY SAMPLED INTERVALS	100.00
AVERAGE TOTAL RESPONSE TIME	0:01.57
TOTAL NO. OF RESPONSE EVENTS	87
TOTAL NO. OF SAMPLED INTERVALS	2
CUMULATIVE RESPONSE PERCENT	
WITHIN 1.0 SECS	26.43
WITHIN 3.0 SECS	95.40
WITHIN 5.0 SECS	100.00
WITHIN 10.0 SECS	100.00
RESPONSE DISTRIBUTION COUNT	
UNDER 1.0 SECS	23
BETWEEN 1.0 - 3.0 SECS	60
BETWEEN 3.0 - 5.0 SECS	4
BETWEEN 5.0 - 10.0 SECS	0
OVER 10.0 SECS	0

Figure 3-9. NLDM Service by Terminal (Profile)

3.1.3.1.8 NLDM Service by Performance Class (SNT115)

INTENDED USAGE:

Use this display to quantify the service level the network provides to a given user group identified by the NetView Session Monitor/NLDM Performance Class (PERFCLSS). If the NLDM performance classes conform to the classification specified in the site's service-level agreements, use this display to track your site's adherence to its commitments.

The job that produces this display will not execute unless account code SNTACT4 is set to the value of PERFCLSS for NetView/NLDM or CA NetMaster data. For information on how to define account codes, refer to Section 7.2.

FORMAT:

This display indicates the average and maximum host, network, and total response times for the selected application. In addition, it gives the host, network, and total response distributions. You can see a sample display of the profile report in Figure 3-10.

DATABASE FILE: NVSRTM

DATA ELEMENTS USED:

PERFCLSS	ZONE	NLDRVAL1	NLDRVAL2	NLDRVAL3	NLDRVAL4
RTMPCOBM	RTMAVTTM	RTMPCTR1	RTMPCTR2	RTMPCTR3	RTMPCTR4
RTMTRESC					

CALCULATIONS:

None

USAGE CONSIDERATIONS:

Note that this report is essentially the same as SNT105, which produces a performance class report from the SNTNSV File. We recommend using the NVSRTM File in place of the SNTNSV File with SNT4100 or higher.

You can report on different performance classes by

changing the value of the %SL115 macro in
 prefix.MICS.USER.SOURCE(#SNTRPTS). The default macro
 selects all performance classes.

CA MICS NETWORK COMPONENT

(SNT115) NLDM SERVICE BY PERFORMANCE CLASS: TSO

NETWORK: NETWORK1 SYSTEM: TS02

PRODUCED: AUGUST 7, 2003 ZONE: PRIME TIME

+-----+	
ACTIVITY INDICATORS	08/04/03
+-----+	
TOTAL SERVICE	
OBJECTIVE 80.0% < 1.0	
% MET OVERALL	87.11
% MET BY SAMPLED INTERVALS	49.77
AVERAGE TOTAL RESPONSE TIME	0:00.66
TOTAL NO. OF RESPONSE EVENTS	39,240
TOTAL NO. OF SAMPLED INTERVALS	215
CUMULATIVE RESPONSE PERCENT	
WITHIN 1.0 SECS	87.11
WITHIN 2.0 SECS	93.45
WITHIN 3.0 SECS	96.11
WITHIN 5.0 SECS	98.21
RESPONSE DISTRIBUTION COUNT	
UNDER 1.0 SECS	34,182
BETWEEN 1.0 - 2.0 SECS	2,489
BETWEEN 2.0 - 3.0 SECS	1,041
BETWEEN 3.0 - 5.0 SECS	828
OVER 5.0 SECS	700
+-----+	

Figure 3-10. NLDM Service by Performance Class (Profile)

3.1.3.1.9 NetSpy Service by Application (SNT121)

INTENDED USAGE:

This display is used to quantify the service level provided by the network to a given primary logical unit (PLU). This display is useful for tracking end user response time for particular applications and identifying occurrences of excessive host, network, or total response time.

FORMAT:

This display indicates the average total response times for the selected applications and gives response distributions. A sample display of the profile report is reproduced in Figure 3-11.

DATABASE FILE: SNTNSP

DATA ELEMENTS USED:

PLU	ZONE	NSPRVAL1	NSPRVAL2	NSPRVAL3	NSPRVAL4
NSPAVNTM	NSPAVTTM	NSPPCTR1	NSPPCTR2	NSPPCTR3	NSPPCTR4
NSPTRESC	NSPAVHTM				

CALCULATIONS:

None

USAGE CONSIDERATIONS:

You can vary the PLUs that are reported by changing the value of the %SL121 macro in prefix.MICS.USER.SOURCE(#SNT121). The default macro selects all PLUs.

CA MICS NETWORK COMPONENT		
(SNT121) NETSPY SERVICE BY APPLICATION: CICS		
NETWORK: NETWORK1 SYSTEM: SYSA		
PRODUCED: JANUARY 21, 2004 ZONE: PRIME TIME		
+-----+		
ACTIVITY INDICATORS	01/20/04	
+-----+		
HOST SERVICE		
AVERAGE HOST RESPONSE TIME	0:00.98	
MAXIMUM HOST RESPONSE TIME	1:54.29	
NO. OF HOST RESPONSES	312,067	
NETWORK SERVICE		
AVERAGE NETWORK RESPONSE TIME	0:00.98	
MAXIMUM NETWORK RESPONSE TIME	1:09.01	
NO. OF NETWORK RESPONSES	283,009	
TOTAL SERVICE		
AVERAGE TOTAL RESPONSE TIME	0:01.96	
PERCENT WITHIN 1 SECS	39.66	
PERCENT WITHIN 3 SECS	71.73	
PERCENT WITHIN 5 SECS	83.33	
PERCENT WITHIN 10 SECS	88.95	
TOTAL NO. OF RESPONSES	312,067	
RESPONSES W/TOTAL RESP TIME		
GT THAN 10 SECS	34,481	
+-----+		

Figure 3-11. NetSpy Service by Application (Profile)

3.1.3.1.10 NetSpy Service by Terminal (SNT122)

INTENDED USAGE:

This display is used to quantify the service level provided by the network to a given terminal (SLU) when in session with a particular application (PLU). This display is useful for tracking end-user response time for individual terminals and identifying occurrences of excessive host, network, or total response time.

FORMAT:

This display indicates the average total response times for the selected terminal and application, and gives response distributions. The report header will also identify the type of application session data based upon the NSSLU62F flag element. You can see sample displays of profile and trend reports in these figures:

- o 3-12 3-12A (LU6.2 Profile/Trend Reports)
- o 3-12B 3-12C (NON-LU6.2 Profile/Trend Reports)

DATABASE FILE: SNTNSS

DATA ELEMENTS USED:

PLU	SLU	ZONE	NSSRVAL1	NSSRVAL2	NSSRVAL3
NSSRVAL4	NSSAVHTM	NSSAVTTM	NSSPCTR1	NSSPCTR2	NSSPCTR3
NSSPCTR4	NSSTRESC	NSSAVNTM	NSSNRESC	NSSNRURM	NSSLU62F

CALCULATIONS:

None

USAGE CONSIDERATIONS:

You can vary the SLUs and PLUs that are reported by changing the value of the %SL122 macro in prefix.MICS.USER.SOURCE(#SNT122). The default macro selects all SLU and PLU combinations.

CA MICS NETWORK COMPONENT

(SNT122) NETSPY SERVICE FOR TERMINAL: LU27004X LU62SES=Y

NETWORK: NETWORK1 SYSTEM: NSRA APPLICATION: XCOMJACB
 PRODUCED: OCTOBER 14, 2004 ZONE: PRIME TIME

ACTIVITY INDICATORS		08/22/04
HOST SERVICE		
AVERAGE HOST RESPONSE TIME		0:14.02
MAXIMUM HOST RESPONSE TIME		0:14.02
NO. OF HOST RESPONSES		1
NETWORK SERVICE		
AVERAGE NETWORK RESPONSE TIME		0:10.16
MAXIMUM NETWORK RESPONSE TIME		0:10.16
NO. OF NETWORK RESPONSES		1
TOTAL SERVICE		
AVERAGE TOTAL RESPONSE TIME		0:24.18
TOTAL NO. OF RESPONSES		1
TOTAL NO. OF NETWORK RESPONSE		1
TOTAL NO. OF USER RESPONSES		1
TOTAL RESPONSE DISTRIBUTION		
PERCENT WITHIN	1 SECS	0.00
PERCENT WITHIN	1 SECS	0.00
PERCENT WITHIN	1 SECS	0.00
PERCENT WITHIN	2 SECS	0.00
RESPONSES GT THAN	2 SECS	1

Figure 3-12. NetSpy Service by Terminal (Profile)

3.1 Tabular Reports

CA MICS NETWORK COMPONENT (SNT122) NETSPY SERVICE FOR TERMINAL: LU27004X LU62SES=Y NETWORK: NETWORK1 SYSTEM: NSRA APPLICATION: XCOMJACB PRODUCED: OCTOBER 14, 2004 ZONE: PRIME TIME						
ACTIVITY INDICATORS	08/22/04	.	.	AMOUNT OF CHANGE SINCE	PER-PERIOD RATE OF CHANGE SINCE	PERCENTAGE CHANGE SINCE
HOST SERVICE						
AVERAGE HOST RESPONSE TIME	0:14.02					
MAXIMUM HOST RESPONSE TIME	0:14.02					
NO. OF HOST RESPONSES	1					
NETWORK SERVICE						
AVERAGE NETWORK RESPONSE TIME	0:10.16					
MAXIMUM NETWORK RESPONSE TIME	0:10.16					
NO. OF NETWORK RESPONSES	1					
TOTAL SERVICE						
AVERAGE TOTAL RESPONSE TIME	0:24.18					
TOTAL NO. OF RESPONSES	1					
TOTAL NO. OF NETWORK RESPONSE	1					
TOTAL NO. OF USER RESPONSES	1					
TOTAL RESPONSE DISTRIBUTION						
PERCENT WITHIN 1 SECS	0.00					
PERCENT WITHIN 1 SECS	0.00					
PERCENT WITHIN 1 SECS	0.00					
PERCENT WITHIN 2 SECS	0.00					
RESPONSES GT THAN 2 SECS	1					

Figure 3-12A. NetSpy Service by Terminal (Trend)

CA MICS NETWORK COMPONENT

(SNT122) NETSPY SERVICE FOR TERMINAL: TPPG002 LU62SES=N

NETWORK: NETWORK1 SYSTEM: NSRA APPLICATION: RCMVS26

PRODUCED: OCTOBER 14, 2004 ZONE: PRIME TIME

ACTIVITY INDICATORS		08/22/04
HOST SERVICE		
AVERAGE HOST RESPONSE TIME		0:00.03
MAXIMUM HOST RESPONSE TIME		0:00.66
NO. OF HOST RESPONSES		20
NETWORK SERVICE		
AVERAGE NETWORK RESPONSE TIME		0:00.63
MAXIMUM NETWORK RESPONSE TIME		0:00.98
NO. OF NETWORK RESPONSES		11
TOTAL SERVICE		
AVERAGE TOTAL RESPONSE TIME		0:00.66
TOTAL NO. OF RESPONSES		20
TOTAL NO. OF NETWORK RESPONSE		11
TOTAL NO. OF USER RESPONSES		11
TOTAL RESPONSE DISTRIBUTION		
PERCENT WITHIN 1 SECS		72.73
PERCENT WITHIN 3 SECS		100.00
PERCENT WITHIN 5 SECS		100.00
PERCENT WITHIN 10 SECS		100.00
RESPONSES GT THAN 10 SECS		3

Figure 3-12B. NetSpy Service by Terminal (Profile)

CA MICS NETWORK COMPONENT (SNT122) NETSPY SERVICE FOR TERMINAL: TPPG002 LU62SES=N NETWORK: NETWORK1 SYSTEM: NSRA APPLICATION: RCMVS26 PRODUCED: OCTOBER 14, 2004 ZONE: PRIME TIME						
ACTIVITY INDICATORS	08/22/04	.	.	AMOUNT OF CHANGE SINCE	PER-PERIOD RATE OF CHANGE SINCE	PERCENTAGE CHANGE SINCE
HOST SERVICE						
AVERAGE HOST RESPONSE TIME	0:00.03					
MAXIMUM HOST RESPONSE TIME	0:00.66					
NO. OF HOST RESPONSES	20					
NETWORK SERVICE						
AVERAGE NETWORK RESPONSE TIME	0:00.63					
MAXIMUM NETWORK RESPONSE TIME	0:00.98					
NO. OF NETWORK RESPONSES	11					
TOTAL SERVICE						
AVERAGE TOTAL RESPONSE TIME	0:00.66					
TOTAL NO. OF RESPONSES	20					
TOTAL NO. OF NETWORK RESPONSE	11					
TOTAL NO. OF USER RESPONSES	11					
TOTAL RESPONSE DISTRIBUTION						
PERCENT WITHIN 1 SECS	72.73					
PERCENT WITHIN 3 SECS	100.00					
PERCENT WITHIN 5 SECS	100.00					
PERCENT WITHIN 10 SECS	100.00					
RESPONSES GT THAN 10 SECS	3					

Figure 3-12C. NetSpy Service by Terminal (Trend)

3.1.3.2 Workload Analysis Reports

Workload analysis reports display the use of a given network component. You can produce these reports either in profile format or in trend format. Profile reports display data that is retained in a single cycle of the CA MICS database. Trend reports compare three cycles of data.

You can also produce any report in the sections listed below that contains the data source name Tivoli NetView NLDM from equivalent data collected by the CA NetMaster NTS Product.

The following sections explain the utilization reports in greater detail:

- 1 - NPM Workload by Application (SNT201)
- 2 - NPM Workload by Link (SNT203)
- 3 - NPM/NetSpy Utilization by NCP (SNT208)
- 4 - NPM/NetSpy NCP Utilization by Link (SNT209)
- 5 - NLDM Workload by Application (SNT211)
- 6 - NLDM Workload by Link (SNT212)
- 7 - NLDM Workload by Control Unit (SNT213)
- 8 - NLDM Workload by Terminal (SNT214)
- 9 - NPM/NetSpy NCP Utilization by Link (SNT215)
- 10 - NPM/NetSpy NCP Utilization by Link (SNT216)
- 11 - NetSpy Workload by Application (SNT221)
- 12 - NetSpy Workload by Terminal (SNT222)

3.1.3.2.1 NPM Workload by Application (SNT201)

INTENDED USAGE:

Use this display to quantify the workload volume a given host application imposes on the network. Monitor this report for indications that the maximum supportable utilization level is being reached.

FORMAT:

This display indicates the character and path information unit (PIU) for selected primary logical units (PLUs). You can see sample displays of profile and trend reports in figures 3-13 and 3-13A.

DATABASE FILE: SNTLSY

DATA ELEMENTS USED:

PLU	ZONE	PSYTRESC	PSYAVNFS	PSYAVNFR	PSYAVFMS
PSYAVFMR	PSYNRNFS	PSYNRNFR	PSYNRFMS	PSYNRFMR	
PSYNRPNR	PSYNRPNS	PSYNRPFS	PSYNRPFR		

CALCULATIONS:

$DURATION = (ENDTS - STARTTS)$

$TOTAL\ CONTROL\ BYTES / MIN =$
 $SUM(PSYNRNFR, PSYNRNFS) / (DURATION / 60)$

$CTRL\ BYTES\ SENT / MIN = PSYNRNFS / (DURATION / 60)$

$CTRL\ BYTES\ RECEIVED / MIN = PSYNRNFR / (DURATION / 60)$

$TOTAL\ DATA\ BYTES / MIN =$
 $SUM(PSYNRFMS, PSYNRFMR) / (DURATION / 60)$

$DATA\ BYTES\ SENT / MIN = PSYNRFMS / (DURATION / 60)$

$DATA\ BYTES\ RECEIVED / MIN = PSYNRFMR / (DURATION / 60)$

$TOTAL\ BYTES / MIN =$
 $SUM(PSYNRNFR, PSYNRNFS, PSYNRFMS, PSYNRFMR) / (DURATION / 60)$

TOTAL BYTES SENT / MIN =
SUM(PSYNRNFS,PSYNRFMS) / (DURATION / 60)

TOTAL BYTES RECEIVED / MIN =
SUM(PSYNRNFR,PSYNRFMR) / (DURATION / 60)

TOTAL CTRL PIUS / MIN =
SUM(PSYNRPNR,PSYNRPNS) / (DURATION / 60)

CTRL PIUS SENT / MIN = PSYNRPNS / (DURATION / 60)

CTRL PIUS RECEIVED / MIN = PSYNRPNR / (DURATION / 60)

TOTAL DATA PIUS / MIN =
SUM(PSYNRPFS,PSYNRPFR) / (DURATION / 60)

DATA PIUS SENT / MIN = PSYNRPFS / (DURATION / 60)

DATA PIUS RECEIVED / MIN = PSYNRPFR / (DURATION / 60)

TOTAL PIUS / MIN =
SUM(PSYNRPNR,PSYNRPNS,PSYNRPFS,PSYNRPFR) / (DURATION / 60)

TOTAL PIUS SENT / MIN =
SUM(PSYNRPNS,PSYNRPFS) / (DURATION / 60)

TOTAL PIUS RECEIVED / MIN =
SUM(PSYNRPNR,PSYNRPFR) / (DURATION / 60)

NUMBER OF RESPONSES / MIN = PSYTRESC / (DURATION / 60)

TOTAL BYTES TRANSMITTED =
SUM(PSYNRFMR,PSYNRFMS,PSYNRNFR,PSYNRNFS)

CTRL BYTES TRANSMITTED = SUM(PSYNRNFR,PSYNRNFS)

DATA BYTES TRANSMITTED = SUM(PSYNRFMR,PSYNRFMS)

TOTAL PIUS TRANSMITTED =
SUM(PSYNRPFR,PSYNRPFS,PSYNRPNR,PSYNRPNS)

CTRL PIUS TRANSMITTED = SUM(PSYNRPNR,PSYNRPNS)

DATA PIUS TRANSMITTED = SUM(PSYNRPFR,PSYNRPFS)

AVG BYTES PER RESPONSE =
SUM(PSYNRFMR,PSYNRFMS,PSYNRNFR,PSYNRNFS) / PSYTRESC

AVG PIUS PER RESPONSE =

`SUM(PSYNRPFR,PSYNRPFS,PSYNRPNR,PSYNRPNS) / PSYTRESC`

USAGE CONSIDERATIONS:

You can report on a different number of PLUs by changing the value of the %SL201 macro in `prefix.MICS.USER.SOURCE(#SNTRPTS)`. The default macro selects all PLUs.

CA MICS NETWORK COMPONENT
(SNT201) NPM WORKLOAD BY APPLICATION: CICSPROD
NETWORK: NETWORK1 SYSTEM: 3084
PRODUCED: OCTOBER 20, 2003 ZONE: PRIME TIME

ACTIVITY INDICATORS	10/18/03
THROUGHPUT DATA	
TOTAL CONTROL BYTES / MIN	25.47
CTRL BYTES SENT / MIN	16.65
CTRL BYTES RECEIVED / MIN	8.82
TOTAL DATA BYTES / MIN	47704.17
DATA BYTES SENT / MIN	42385.56
DATA BYTES RECEIVED / MIN	5318.61
TOTAL BYTES / MIN	47729.65
TOTAL BYTES SENT / MIN	42402.21
TOTAL BYTES RECEIVED / MIN	5327.43
TOTAL CTRL PIUS / MIN	4.29
CTRL PIUS SENT / MIN	2.13
CTRL PIUS RECEIVED / MIN	2.16
TOTAL DATA PIUS / MIN	145.94
DATA PIUS SENT / MIN	69.13
DATA PIUS RECEIVED / MIN	76.81
TOTAL PIUS / MIN	150.23
TOTAL PIUS SENT / MIN	71.26
TOTAL PIUS RECEIVED / MIN	78.97
NUMBER OF RESPONSES / MIN	66.36
WORKLOAD STATISTICS	
TOTAL BYTES TRANSMITTED	14,604,476
CTRL BYTES TRANSMITTED	7,794
DATA BYTES TRANSMITTED	14,596,682
TOTAL PIUS TRANSMITTED	45,968
CTRL PIUS TRANSMITTED	1,312
DATA PIUS TRANSMITTED	44,656
TOTAL RESPONSES	20,304
AVG BYTES PER CNTL PIU SENT	7.82
AVG BYTES PER CNTL PIU REC'D	4.08
AVG BYTES PER DATA PIU SENT	613.15
AVG BYTES PER DATA PIU REC'D	69.24

	AVG BYTES PER RESPONSE	719.29	
	AVG PIUS PER RESPONSE	2.26	
+-----+-----+-----+			

Figure 3-13. NPM Workload by Application (Profile)

CA MICS NETWORK COMPONENT (SNT201) NPM WORKLOAD BY APPLICATION: CICSPROD NETWORK: NETWORK1 SYSTEM: 3084 PRODUCED: OCTOBER 20, 2003 ZONE: PRIME TIME						
ACTIVITY INDICATORS	10/18/03	10/17/03	10/16/03	AMOUNT OF CHANGE SINCE 10/16/03	PER-PERIOD RATE OF CHANGE SINCE 10/16/03	PERCENTAGE CHANGE SINCE 10/16/03
THROUGHPUT DATA						
TOTAL CONTROL BYTES / MIN	25.47	35.69	20.80	4.67	2.34	22.47
CTRL BYTES SENT / MIN	16.65	24.35	13.78	2.87	1.43	20.83
CTRL BYTES RECEIVED / MIN	8.82	11.33	7.02	1.80	0.90	25.70
TOTAL DATA BYTES / MIN	47704.17	55749.70	40053.24	7650.93	3825.47	19.10
DATA BYTES SENT / MIN	42385.56	48636.54	35285.18	7100.38	3550.19	20.12
DATA BYTES RECEIVED / MIN	5318.61	7113.15	4768.06	550.55	275.28	11.55
TOTAL BYTES / MIN	47729.65	55785.38	40074.04	7655.61	3827.80	19.10
TOTAL BYTES SENT / MIN	42402.21	48660.90	35298.96	7103.25	3551.62	20.12
TOTAL BYTES RECEIVED / MIN	5327.43	7124.49	4775.08	552.36	276.18	11.57
TOTAL CTRL PIUS / MIN	4.29	5.44	3.39	0.90	0.45	26.64
CTRL PIUS SENT / MIN	2.13	2.69	1.68	0.45	0.23	26.90
CTRL PIUS RECEIVED / MIN	2.16	2.75	1.71	0.45	0.23	26.39
TOTAL DATA PIUS / MIN	145.94	165.83	119.70	26.25	13.12	21.93
DATA PIUS SENT / MIN	69.13	77.07	56.03	13.10	6.55	23.39
DATA PIUS RECEIVED / MIN	76.81	88.76	63.67	13.14	6.57	20.64
TOTAL PIUS / MIN	150.23	171.27	123.08	27.15	13.57	22.06
TOTAL PIUS SENT / MIN	71.26	79.76	57.70	13.55	6.78	23.49
TOTAL PIUS RECEIVED / MIN	78.97	91.50	65.38	13.60	6.80	20.79
NUMBER OF RESPONSES / MIN	66.36	73.40	53.94	12.42	6.21	23.02
WORKLOAD STATISTICS						
TOTAL BYTES TRANSMITTED	14,604,476	17,069,398	12,261,988	2,342,488	1171244.00	19.10
CTRL BYTES TRANSMITTED	7,794	10,920	6,364	1,430	715.00	22.47
DATA BYTES TRANSMITTED	14,596,682	17,058,478	12,255,624	2,341,058	1170529.00	19.10
TOTAL PIUS TRANSMITTED	45,968	52,405	37,661	8,307	4153.50	22.06
CTRL PIUS TRANSMITTED	1,312	1,664	1,036	276	138.00	26.64
DATA PIUS TRANSMITTED	44,656	50,741	36,625	8,031	4015.50	21.93
TOTAL RESPONSES	20,304	22,458	16,504	3,800	1900.00	23.02
AVG BYTES PER CNTL PIU SENT	7.82	9.05	8.22	-0.39	-0.20	-4.79
AVG BYTES PER CNTL PIU REC'D	4.08	4.12	4.11	-0.02	-0.01	-0.54
AVG BYTES PER DATA PIU SENT	613.15	631.05	629.80	-16.65	-8.33	-2.64
AVG BYTES PER DATA PIU REC'D	69.24	80.14	74.89	-5.65	-2.82	-7.54
AVG BYTES PER RESPONSE	719.29	760.06	742.97	-23.68	-11.84	-3.19
AVG PIUS PER RESPONSE	2.26	2.33	2.28	-0.02	-0.01	-0.79

Figure 3-13A. NPM Workload by Application (Trend)

3.1.3.2.2 NPM Workload By Link (SNT203)

INTENDED USAGE:

Use this display to quantify the workload volume imposed on the network by the devices attached to a given boundary link. Monitor this report for indications that the maximum supportable link utilization is being reached.

FORMAT:

This display indicates the character and path information unit (PIU) throughput of selected links. You can see sample displays of profile and trend reports in Figures 3-14 and 3-14A.

DATABASE FILE: SNTNPL

DATA ELEMENTS USED:

PLU	ZONE	NPLTRES	NPLAVNFS	NPLAVNFR	NPLAVFMS
NPLAVFMR	NPLNRNFS	NPLNRNFR	NPLNRFMS	NPLNRFMR	
NPLNRPNR	NPLNRPNS	NPLNRPFS	NPLNRPFR		

CALCULATIONS:

$DURATION = (ENDTS - STARTTS)$

$TOTAL\ CONTROL\ BYTES / MIN =$
 $SUM(NPLNRNFR, NPLNRNFS) / (DURATION / 60)$

$CTRL\ BYTES\ SENT / MIN = NPLNRNFS / (DURATION / 60)$

$CTRL\ BYTES\ RECEIVED / MIN = NPLNRNFR / (DURATION / 60)$

$TOTAL\ DATA\ BYTES / MIN =$
 $SUM(NPLNRFMS, NPLNRFMR) / (DURATION / 60)$

$DATA\ BYTES\ SENT / MIN = NPLNRFMS / (DURATION / 60)$

$DATA\ BYTES\ RECEIVED / MIN = NPLNRFMR / (DURATION / 60)$

$TOTAL\ BYTES / MIN =$
 $SUM(NPLNRNFR, NPLNRNFS, NPLNRFMS, NPLNRFMR) / (DURATION / 60)$

TOTAL BYTES SENT / MIN =
$$\text{SUM}(\text{NPLNRNFS}, \text{NPLNRFMS}) / (\text{DURATION} / 60)$$

TOTAL BYTES RECEIVED / MIN =
$$\text{SUM}(\text{NPLNRNFR}, \text{NPLNRFMR}) / (\text{DURATION} / 60)$$

TOTAL CTRL PIUS / MIN =
$$\text{SUM}(\text{NPLNRPNR}, \text{NPLNRPNS}) / (\text{DURATION} / 60)$$

CTRL PIUS SENT / MIN = $\text{NPLNRPNS} / (\text{DURATION} / 60)$

CTRL PIUS RECEIVED / MIN = $\text{NPLNRPNR} / (\text{DURATION} / 60)$

TOTAL DATA PIUS / MIN =
$$\text{SUM}(\text{NPLNRPFS}, \text{NPLNRPFR}) / (\text{DURATION} / 60)$$

DATA PIUS SENT / MIN = $\text{NPLNRPFS} / (\text{DURATION} / 60)$

DATA PIUS RECEIVED / MIN = $\text{NPLNRPFR} / (\text{DURATION} / 60)$

TOTAL PIUS / MIN =
$$\text{SUM}(\text{NPLNRPNR}, \text{NPLNRPNS}, \text{NPLNRPFS}, \text{NPLNRPFR}) / (\text{DURATION} / 60)$$

TOTAL PIUS SENT / MIN =
$$\text{SUM}(\text{NPLNRPNS}, \text{NPLNRPFS}) / (\text{DURATION} / 60)$$

TOTAL PIUS RECEIVED / MIN =
$$\text{SUM}(\text{NPLNRPNR}, \text{NPLNRPFR}) / (\text{DURATION} / 60)$$

NUMBER OF RESPONSES / MIN = $\text{NPLTRESC} / (\text{DURATION} / 60)$

TOTAL BYTES TRANSMITTED =
$$\text{SUM}(\text{NPLNRFMR}, \text{NPLNRFMS}, \text{NPLNRNFR}, \text{NPLNRNFS})$$

CTRL BYTES TRANSMITTED = $\text{SUM}(\text{NPLNRNFR}, \text{NPLNRNFS})$

DATA BYTES TRANSMITTED = $\text{SUM}(\text{NPLNRFMR}, \text{NPLNRFMS})$

TOTAL PIUS TRANSMITTED =
$$\text{SUM}(\text{NPLNRPFR}, \text{NPLNRPFS}, \text{NPLNRPNR}, \text{NPLNRPNS})$$

CTRL PIUS TRANSMITTED = $\text{SUM}(\text{NPLNRPNR}, \text{NPLNRPNS})$

DATA PIUS TRANSMITTED = $\text{SUM}(\text{NPLNRPFR}, \text{NPLNRPFS})$

AVG BYTES PER RESPONSE =
$$\text{SUM}(\text{NPLNRFMR}, \text{NPLNRFMS}, \text{NPLNRNFR}, \text{NPLNRNFS}) / \text{NPLTRESC}$$

AVG PIUS PER RESPONSE =

SUM(NPLNRPFR,NPLNRPFS,NPLNRPNR,NPLNRPNS) / NPLTRESC

USAGE CONSIDERATIONS:

You can vary the number of links for which reports are produced by changing the value of the %SL203 macro in prefix.MICS.USER.SOURCE(#SNTRPTS). The default macro selects all links.

CA MICS NETWORK COMPONENT
 (SNT203) NPM WORKLOAD BY LINK: ABLINK1
 NETWORK: NETWORK1 SYSTEM: 3084
 PRODUCED: OCTOBER 20, 2003 ZONE: PRIME TIME

ACTIVITY INDICATORS	10/17/03
THROUGHPUT DATA	
TOTAL CONTROL BYTES / MIN	81.07
CTRL BYTES SENT / MIN	37.91
CTRL BYTES RECEIVED / MIN	43.16
TOTAL DATA BYTES / MIN	5436.32
DATA BYTES SENT / MIN	5127.67
DATA BYTES RECEIVED / MIN	308.65
TOTAL BYTES / MIN	5517.39
TOTAL BYTES SENT / MIN	5165.58
TOTAL BYTES RECEIVED / MIN	351.81
TOTAL CTRL PIUS / MIN	13.05
CTRL PIUS SENT / MIN	2.42
CTRL PIUS RECEIVED / MIN	10.62
TOTAL DATA PIUS / MIN	13.92
DATA PIUS SENT / MIN	7.59
DATA PIUS RECEIVED / MIN	6.34
TOTAL PIUS / MIN	26.97
TOTAL PIUS SENT / MIN	10.01
TOTAL PIUS RECEIVED / MIN	16.96
NUMBER OF RESPONSES / MIN	5.42
WORKLOAD STATISTICS	
TOTAL BYTES TRANSMITTED	1,520,132
CTRL BYTES TRANSMITTED	22,335
DATA BYTES TRANSMITTED	1,497,797
TOTAL PIUS TRANSMITTED	7,431
CTRL PIUS TRANSMITTED	3,595
DATA PIUS TRANSMITTED	3,836
TOTAL RESPONSES	1,494
AVG BYTES PER CNTL PIU SENT	15.63
AVG BYTES PER CNTL PIU REC'D	4.06
AVG BYTES PER DATA PIU SENT	675.96
AVG BYTES PER DATA PIU REC'D	48.70

AVG BYTES PER RESPONSE	1017.49
AVG PIUS PER RESPONSE	4.97

Figure 3-14. NPM Workload by Link (Profile)

CA MICS NETWORK COMPONENT						
(SNT203) NPM WORKLOAD BY LINK: ABLINK1						
NETWORK: NETWORK1 SYSTEM: 3084						
PRODUCED: OCTOBER 20, 2003 ZONE: PRIME TIME						
ACTIVITY INDICATORS	10/17/03	10/16/03	10/15/03	AMOUNT OF CHANGE SINCE 10/15/03	PER-PERIOD RATE OF CHANGE SINCE 10/15/03	PERCENTAGE CHANGE SINCE 10/15/03
THROUGHPUT DATA						
TOTAL CONTROL BYTES / MIN	81.07	107.02	111.93	-30.87	-15.43	-27.58
CTRL BYTES SENT / MIN	37.91	51.87	45.30	-7.39	-3.70	-16.32
CTRL BYTES RECEIVED / MIN	43.16	55.14	66.64	-23.48	-11.74	-35.23
TOTAL DATA BYTES / MIN	5436.32	6937.91	9101.64	-3665.32	-1832.66	-40.27
DATA BYTES SENT / MIN	5127.67	6144.79	8807.00	-3679.33	-1839.66	-41.78
DATA BYTES RECEIVED / MIN	308.65	793.13	294.64	14.01	7.00	4.75
TOTAL BYTES / MIN	5517.39	7044.93	9213.58	-3696.19	-1848.09	-40.12
TOTAL BYTES SENT / MIN	5165.58	6196.66	8852.30	-3686.72	-1843.36	-41.65
TOTAL BYTES RECEIVED / MIN	351.81	848.27	361.28	-9.47	-4.73	-2.62
TOTAL CTRL PIUS / MIN	13.05	16.70	20.22	-7.17	-3.59	-35.48
CTRL PIUS SENT / MIN	2.42	3.46	2.81	-0.38	-0.19	-13.66
CTRL PIUS RECEIVED / MIN	10.62	13.24	17.41	-6.79	-3.40	-38.99
TOTAL DATA PIUS / MIN	13.92	18.45	26.18	-12.26	-6.13	-46.82
DATA PIUS SENT / MIN	7.59	9.19	19.49	-11.90	-5.95	-61.08
DATA PIUS RECEIVED / MIN	6.34	9.26	6.69	-0.35	-0.18	-5.30
TOTAL PIUS / MIN	26.97	35.15	46.40	-19.43	-9.72	-41.88
TOTAL PIUS SENT / MIN	10.01	12.65	22.30	-12.29	-6.14	-55.11
TOTAL PIUS RECEIVED / MIN	16.96	22.50	24.11	-7.15	-3.57	-29.64
NUMBER OF RESPONSES / MIN	5.42	6.77	6.20	-0.78	-0.39	-12.57
WORKLOAD STATISTICS						
TOTAL BYTES TRANSMITTED	1,520,132	1,687,378	1,824,288	-304,156	-152078.00	-16.67
CTRL BYTES TRANSMITTED	22,335	25,632	22,163	172	86.00	0.78
DATA BYTES TRANSMITTED	1,497,797	1,661,746	1,802,125	-304,328	-152164.00	-16.89
TOTAL PIUS TRANSMITTED	7,431	8,418	9,188	-1,757	-878.50	-19.12
CTRL PIUS TRANSMITTED	3,595	4,000	4,004	-409	-204.50	-10.21
DATA PIUS TRANSMITTED	3,836	4,418	5,184	-1,348	-674.00	-26.00
TOTAL RESPONSES	1,494	1,622	1,228	266	133.00	21.66
AVG BYTES PER CNTL PIU SENT	15.63	15.00	16.13	-0.50	-0.25	-3.08
AVG BYTES PER CNTL PIU REC'D	4.06	4.16	3.83	0.24	0.12	6.17
AVG BYTES PER DATA PIU SENT	675.96	668.69	451.88	224.09	112.04	49.59
AVG BYTES PER DATA PIU REC'D	48.70	85.69	44.03	4.68	2.34	10.62
AVG BYTES PER RESPONSE	1017.49	1040.31	1485.58	-468.09	-234.04	-31.51
AVG PIUS PER RESPONSE	4.97	5.19	7.48	-2.51	-1.25	-33.52

Figure 3-14A. NPM Workload by Link (Trend)

3.1.3.2.3 NPM/NetSpy Utilization by NCP (SNT208)

SOURCE:

The source for this report can be either Tivoli NetView NPM Network data or CA NetSpy NCP interface data.

INTENDED USAGE:

Use this display to identify and quantify potential capacity-related bottlenecks in the network's "backbone" NCPs. Queuing bottlenecks (pacing, slowdown, and so on) frequently occur when the communications processor (37xx or equivalent) supporting the NCP becomes overloaded. You can monitor this report for indications that the maximum supportable utilization level is being reached.

FORMAT:

This display indicates the throughput and utilization of selected NCPs in the network. You can see sample displays of profile and trend reports in Figures 3-15, 3-15A, 3-16, and 3-16A.

DATABASE FILE: SNTNAF

DATA ELEMENTS USED:

NAFMNHQL	NAFAVHQL	NAFMXHQL	NAFMNIQL	NAFAVIQL	NAFMXIQL
NAFMXANP	NAFMNFB	NAFMXFBH	NAFMNFBQ	NAFAVFBQ	NAFMXFBQ
NAFAVSFB	NAFPCCCU	NAFPCTIS			

CALCULATIONS:

None

USAGE CONSIDERATIONS:

You can vary the number of NCPs for which reports are produced by changing the value of the %SL208 macro in prefix.MICS.USER.SOURCE(#SNT208). The default macro selects all NCPs.

CA MICS NETWORK COMPONENT		
(SNT208) NPM UTILIZATION FOR NCP: NCP2303		
NETWORK: NETWORK1 SYSTEM: S002		
PRODUCED: APRIL 4, 2004 ZONE: PRIME TIME		
+-----+		
ACTIVITY INDICATORS	04/01/04	
+-----+		
QUEUEING STATISTICS		
MIN CHANNEL HOLD QUEUE LENGTH	6	
AVG CHANNEL HOLD QUEUE LENGTH	16.74	
MAX CHANNEL HOLD QUEUE LENGTH	27	
MIN CHANNEL INTERMED Q LENGTH	3	
AVG CHANNEL INTERMED Q LENGTH	12.74	
MAX CHANNEL INTERMED Q LENGTH	26	
BUFFER STATISTICS		
MAX AVAILABLE NCP BUFFERS	5,675	
FREE BUFFER LOW-WATER MARK	4,508	
FREE BUFFER HIGH-WATER MARK	5,585	
MIN FREE BUFFER QUEUE LENGTH	5,528	
AVG FREE BUFFER QUEUE LENGTH	5,425	
MAX FREE BUFFER QUEUE LENGTH	5,309	
AVG FREE BUFFERS AT SLOWDOWN	708	
BUFFER STATISTICS		
PERCENT CCU UTILIZATION	86.05	
PERCENT TIME IN SLOWDOWN	0.00	
+-----+		

Figure 3-15. NPM Utilization by NCP (Profile)

CA MICS NETWORK COMPONENT						
(SNT208) NPM UTILIZATION FOR NCP: NCP2303						
NETWORK: NETWORK1 SYSTEM: S002						
PRODUCED: APRIL 4, 2004 ZONE: PRIME TIME						
ACTIVITY INDICATORS	04/01/04	03/31/04		AMOUNT OF CHANGE SINCE	PER-PERIOD RATE OF CHANGE SINCE	PERCENTAGE CHANGE SINCE
QUEUEING STATISTICS						
MIN CHANNEL HOLD QUEUE LENGTH	6	10				
AVG CHANNEL HOLD QUEUE LENGTH	16.74	15.14				
MAX CHANNEL HOLD QUEUE LENGTH	27	20				
MIN CHANNEL INTERMED Q LENGTH	3	10				
AVG CHANNEL INTERMED Q LENGTH	12.74	13.43				
MAX CHANNEL INTERMED Q LENGTH	26	21				
BUFFER STATISTICS						
MAX AVAILABLE NCP BUFFERS	5,675	5,675				
FREE BUFFER LOW-WATER MARK	4,508	5,114				
FREE BUFFER HIGH-WATER MARK	5,585	5,568				
MIN FREE BUFFER QUEUE LENGTH	5,528	5,496				
AVG FREE BUFFER QUEUE LENGTH	5,425	5,413				
MAX FREE BUFFER QUEUE LENGTH	5,309	5,345				
AVG FREE BUFFERS AT SLOWDOWN	708	708				
BUFFER STATISTICS						
PERCENT CCU UTILIZATION	86.05	83.04				
PERCENT TIME IN SLOWDOWN	0.00	0.00				

Figure 3-15A. NPM Utilization by NCP (Trend)

CA MICS NETWORK COMPONENT

(SNT208) NETSPY UTILIZATION FOR NCP: N059405

NETWORK: NETWORK1 SYSTEM: S002

PRODUCED: APRIL 4, 2004 ZONE: NON PRIME

ACTIVITY INDICATORS		03/24/04
QUEUEING STATISTICS		
MIN CHANNEL HOLD QUEUE LENGTH	1	
AVG CHANNEL HOLD QUEUE LENGTH	2.40	
MAX CHANNEL HOLD QUEUE LENGTH	5	
MIN CHANNEL INTERMED Q LENGTH	1	
AVG CHANNEL INTERMED Q LENGTH	1.07	
MAX CHANNEL INTERMED Q LENGTH	2	
BUFFER STATISTICS		
MAX AVAILABLE NCP BUFFERS	24,985	
FREE BUFFER LOW-WATER MARK	24,593	
FREE BUFFER HIGH-WATER MARK	24,854	
MIN FREE BUFFER QUEUE LENGTH	24,852	
AVG FREE BUFFER QUEUE LENGTH	24,834	
MAX FREE BUFFER QUEUE LENGTH	24,778	
AVG FREE BUFFERS AT SLOWDOWN	3,122	
BUFFER STATISTICS		
PERCENT CCU UTILIZATION	16.91	
PERCENT TIME IN SLOWDOWN	0.00	

Figure 3-16. NetSpy Utilization by NCP (Profile)

CA MICS NETWORK COMPONENT							
(SNT208) NETSPY UTILIZATION FOR NCP: N059405							
NETWORK: NETWORK1 SYSTEM: S002							
PRODUCED: APRIL 4, 2004 ZONE: NON PRIME							
ACTIVITY INDICATORS	03/24/04	03/23/04	03/22/04	AMOUNT OF CHANGE SINCE 03/22/04	PER-PERIOD RATE OF CHANGE SINCE 03/22/04	PERCENTAGE CHANGE SINCE 03/22/04	
QUEUEING STATISTICS							
MIN CHANNEL HOLD QUEUE LENGTH	1	2	2	-1	-0.50	-50.00	
AVG CHANNEL HOLD QUEUE LENGTH	2.40	3.00	2.58	-0.18	-0.09	-6.87	
MAX CHANNEL HOLD QUEUE LENGTH	5	5	5	0	0.00	0.00	
MIN CHANNEL INTERMED Q LENGTH	1	1	1	0	0.00	0.00	
AVG CHANNEL INTERMED Q LENGTH	1.07	1.94	2.23	-1.16	-0.58	-52.18	
MAX CHANNEL INTERMED Q LENGTH	2	4	5	-3	-1.50	-60.00	
BUFFER STATISTICS							
MAX AVAILABLE NCP BUFFERS	24,985	24,985	24,985	0	0.00	0.00	
FREE BUFFER LOW-WATER MARK	24,593	24,513	24,540	53	26.50	0.22	
FREE BUFFER HIGH-WATER MARK	24,854	24,859	24,860	-6	-3.00	-0.02	
MIN FREE BUFFER QUEUE LENGTH	24,852	24,858	24,859	-7	-3.50	-0.03	
AVG FREE BUFFER QUEUE LENGTH	24,834	24,833	24,836	-2	-1.00	-0.01	
MAX FREE BUFFER QUEUE LENGTH	24,778	24,764	24,787	-9	-4.50	-0.04	
AVG FREE BUFFERS AT SLOWDOWN	3,122	3,122	3,122	0	0.00	0.00	
BUFFER STATISTICS							
PERCENT CCU UTILIZATION	16.91	18.19	20.55	-3.64	-1.82	-17.71	
PERCENT TIME IN SLOWDOWN	0.00	0.00	0.00	0.00	0.00		

Figure 3-16A. NetSpy Utilization by NCP (Trend)

3.1.3.2.4 NPM/NetSpy NCP Utilization by Link (SNT209)

SOURCE:

The source for this report can be either Tivoli NetView NPM Network data or CA NetSpy NCP interface data.

INTENDED USAGE:

Use this display to identify and quantify potential network link over-utilization conditions.

FORMAT:

This display indicates the workload and utilization of selected links supported by each NCP. The report header will also identify the type of link data based upon the DATATYPE element. You can see sample displays of profile and trend reports reproduced in these figures:

- o 3-17 3-17A (NPM Link)
- o 3-17B 3-17C (NPM BSCN Link)
- o 3-18 3-18A (CA NetSpy Link)

DATABASE FILE: SNTNCL

DATA ELEMENTS USED:

NETNAME	ZONE	NCLNRPIU	NCLPCLBS	LINKSPD	DATATYPE
NCLPMCHS	NCLPMCHR	NCLPMMSS	NCLPMSR	NCLNRCHS	NCLNRCHR
NCLNMSS	NCLNRMSR	NCLPMTPL	NCLNRTPL	NCLNRPPL	NCLNRERR

CALCULATIONS:

BYTE THROUGHPUT / MIN =

$$\text{SUM}(\text{NCLNRCHR}, \text{NCLNRCHS}) / \text{DURATION} / 60$$

MESSAGE THROUGHPUT / MIN = $\text{SUM}(\text{NCLNRMSR}, \text{NCLNMSS})$

TOTAL BYTES TRANSMITTED = $\text{SUM}(\text{NCLNRCHR}, \text{NCLNRCHS})$

TOTAL MESSAGES TRANSMITTED = $\text{SUM}(\text{NCLNMSS}, \text{NCLNRMSR})$

AVERAGE WAIT FOR POLL (SECS) =

$$((\text{DURATION} / 60) / \text{NCLNRTPL}) / 2$$

PERCENT POSITIVE POLLS = $(\text{NCLNRPPL}/\text{NCLNRTPL}) * 100$

RETRANSMISSION PERCENTAGE =
 $(\text{NCLNRPIU}/\text{SUM}(\text{NCLNRMSS}, \text{NCLNRMSR})) * 100$

NUMBER OF MESSAGES PER ERROR =
 $\text{SUM}(\text{NCLNRMSS}, \text{NCLNRMSR})/\text{NCLNRERR}$

PERCENT LINK UTILIZATION =
 $((\text{NCLNRCHR} + \text{NCLNRCHS})/(\text{NCLNRRLS}/10)) * (\text{ENDTS} - \text{STARTTS})) * 100$

USAGE CONSIDERATIONS:

You can vary the number of links for which reports are produced by changing the value of the %SL209 macro in prefix.MICS.USER.SOURCE(#SNTRPTS). The default macro selects all links.

CA MICS NETWORK COMPONENT

(SNT209) NPM NCP UTILIZATION FOR LINK: LI24078

NETWORK: NETWORK1 SYSTEM: S002

PRODUCED: APRIL 6, 2004 ZONE: PRIME TIME

ACTIVITY INDICATORS		04/06/04
DATA TRANSMISSION		
BYTE THROUGHPUT / MIN		32346.98
BYTES SENT / MIN		23706.64
BYTES RECEIVED / MIN		8640.34
MESSAGE THROUGHPUT / MIN		91.43
MESSAGES SENT / MIN		70.41
MESSAGES RECEIVED / MIN		21.02
TOTAL BYTES TRANSMITTED		11,159,761
BYTES SENT		8,178,829
BYTES RECEIVED		2,980,932
TOTAL MESSAGES TRANSMITTED		31,545
MESSAGES SENT		24,293
MESSAGES RECEIVED		7,252
POLLING DATA		
AVERAGE POLLING RATE / MIN		1406.91
AVERAGE WAIT FOR POLL (SECS)		0.00
PERCENT POSITIVE POLLS		1.49
TOTAL POLL COUNT		485,386
POSITIVE POLL COUNT		7,249
ERROR DATA		
RETRANSMISSION PERCENTAGE		0.02
NUMBER OF MESSAGES PER ERROR		15772.50
ERROR COUNT		2
RETRANSMISSION COUNT		7
UTILIZATION DATA		
PERCENT LINK UTILIZATION		44.93
LINK SPEED (BITS/SECOND)		9,600

Figure 3-17. NPM NCP Utilization by Link (Profile)

CA MICS NETWORK COMPONENT						
(SNT209) NPM NCP UTILIZATION FOR LINK: LI24078						
NETWORK: NETWORK1 SYSTEM: NPM4						
PRODUCED: APRIL 6, 2004 ZONE: PRIME TIME						
ACTIVITY INDICATORS	04/06/04	04/05/04		AMOUNT OF CHANGE SINCE	PER-PERIOD RATE OF CHANGE SINCE	PERCENTAGE CHANGE SINCE
DATA TRANSMISSION						
BYTE THROUGHPUT / MIN	32346.98	24691.25				
BYTES SENT / MIN	23706.64	14431.52				
BYTES RECEIVED / MIN	8640.34	10259.73				
MESSAGE THROUGHPUT / MIN	91.43	25.07				
MESSAGES SENT / MIN	70.41	19.50				
MESSAGES RECEIVED / MIN	21.02	5.57				
TOTAL BYTES TRANSMITTED	11,159,761	2,222,254				
BYTES SENT	8,178,829	1,298,861				
BYTES RECEIVED	2,980,932	923,393				
TOTAL MESSAGES TRANSMITTED	31,545	2,256				
MESSAGES SENT	24,293	1,755				
MESSAGES RECEIVED	7,252	501				
POLLING DATA						
AVERAGE POLLING RATE / MIN	1406.91	1701.56				
AVERAGE WAIT FOR POLL (SECS)	0.00	0.00				
PERCENT POSITIVE POLLS	1.49	0.33				
TOTAL POLL COUNT	485,386	153,143				
POSITIVE POLL COUNT	7,249	501				
ERROR DATA						
RETRANSMISSION PERCENTAGE	0.02	0.00				
NUMBER OF MESSAGES PER ERROR	15772.50					
ERROR COUNT	2	0				
RETRANSMISSION COUNT	7	0				
UTILIZATION DATA						
PERCENT LINK UTILIZATION	44.93	34.29				
LINK SPEED (BITS/SECOND)	9,600	9,600				

Figure 3-17A. NPM NCP Utilization by Link (Trend)

CA MICS NETWORK COMPONENT

(SNT209) NPM NCP UTILIZATION FOR BSCN LINK: LI24095

NETWORK: NETWORK1 SYSTEM: S002
 PRODUCED: APRIL 6, 2004 ZONE: PRIME TIME

ACTIVITY INDICATORS	04/01/04
DATA TRANSMISSION	
BYTE THROUGHPUT / MIN	1238.55
BYTES SENT / MIN	923.71
BYTES RECEIVED / MIN	314.84
MESSAGE THROUGHPUT / MIN	0.39
MESSAGES SENT / MIN	0.00
MESSAGES RECEIVED / MIN	0.39
TOTAL BYTES TRANSMITTED	353,001
BYTES SENT	263,268
BYTES RECEIVED	89,733
TOTAL MESSAGES TRANSMITTED	112
MESSAGES SENT	0
MESSAGES RECEIVED	112
POLLING DATA	
AVERAGE POLLING RATE / MIN	52.36
AVERAGE WAIT FOR POLL (SECS)	0.01
PERCENT POSITIVE POLLS	1.09
TOTAL POLL COUNT	14,923
POSITIVE POLL COUNT	162
ERROR DATA	
RETRANSMISSION PERCENTAGE	171.43
NUMBER OF MESSAGES PER ERROR	0.05
ERROR COUNT	2,090
RETRANSMISSION COUNT	192
UTILIZATION DATA	
PERCENT LINK UTILIZATION	1.72
LINK SPEED (BITS/SECOND)	9,600

Figure 3-17B. NPM NCP Utilization by Link (Profile)

CA MICS NETWORK COMPONENT						
(SNT209) NPM NCP UTILIZATION FOR BSCN LINK: LI24095						
NETWORK: NETWORK1 SYSTEM: S002						
PRODUCED: APRIL 4, 2004 ZONE: PRIME TIME						
ACTIVITY INDICATORS	04/01/04	.	.	AMOUNT OF CHANGE SINCE	PER-PERIOD RATE OF CHANGE SINCE	PERCENTAGE CHANGE SINCE
DATA TRANSMISSION						
BYTE THROUGHPUT / MIN	1238.55					
BYTES SENT / MIN	923.71					
BYTES RECEIVED / MIN	314.84					
MESSAGE THROUGHPUT / MIN	0.39					
MESSAGES SENT / MIN	0.00					
MESSAGES RECEIVED / MIN	0.39					
TOTAL BYTES TRANSMITTED	353,001					
BYTES SENT	263,268					
BYTES RECEIVED	89,733					
TOTAL MESSAGES TRANSMITTED	112					
MESSAGES SENT	0					
MESSAGES RECEIVED	112					
POLLING DATA						
AVERAGE POLLING RATE / MIN	52.36					
AVERAGE WAIT FOR POLL (SECS)	0.01					
PERCENT POSITIVE POLLS	1.09					
TOTAL POLL COUNT	14,923					
POSITIVE POLL COUNT	162					
ERROR DATA						
RETRANSMISSION PERCENTAGE	171.43					
NUMBER OF MESSAGES PER ERROR	0.05					
ERROR COUNT	2,090					
RETRANSMISSION COUNT	192					
UTILIZATION DATA						
PERCENT LINK UTILIZATION	1.72					
LINK SPEED (BITS/SECOND)	9,600					

Figure 3-17C. NPM NCP Utilization by Link (Trend)

CA MICS NETWORK COMPONENT

(SNT209) NETSPY NCP UTILIZATION FOR LINK: L1306

NETWORK: NETWORK1 SYSTEM: S002

PRODUCED: APRIL 4, 2004 ZONE: PRIME TIME

ACTIVITY INDICATORS	03/24/04
DATA TRANSMISSION	
BYTE THROUGHPUT / MIN	4623.78
BYTES SENT / MIN	3271.80
BYTES RECEIVED / MIN	1351.98
MESSAGE THROUGHPUT / MIN	9.67
MESSAGES SENT / MIN	6.52
MESSAGES RECEIVED / MIN	3.14
TOTAL BYTES TRANSMITTED	2,635,776
BYTES SENT	1,865,084
BYTES RECEIVED	770,692
TOTAL MESSAGES TRANSMITTED	5,510
MESSAGES SENT	3,718
MESSAGES RECEIVED	1,792
POLLING DATA	
AVERAGE POLLING RATE / MIN	213.08
AVERAGE WAIT FOR POLL (SECS)	0.00
PERCENT POSITIVE POLLS	1.38
TOTAL POLL COUNT	121,464
POSITIVE POLL COUNT	1,677
ERROR DATA	
RETRANSMISSION PERCENTAGE	1.87
NUMBER OF MESSAGES PER ERROR	21.19
ERROR COUNT	260
RETRANSMISSION COUNT	103
UTILIZATION DATA	
PERCENT LINK UTILIZATION	3.21
LINK SPEED (BITS/SECOND)	19,200

Figure 3-18. NetSpy NCP Utilization by Link (Profile)

CA MICS NETWORK COMPONENT						
(SNT209) NETSPY NCP UTILIZATION FOR LINK: L1306						
NETWORK: NETWORK1 SYSTEM: S002						
PRODUCED: APRIL 4, 2004 ZONE: PRIME TIME						
ACTIVITY INDICATORS	03/24/04	03/23/04	03/22/04	AMOUNT OF CHANGE SINCE 03/22/04	PER-PERIOD RATE OF CHANGE SINCE 03/22/04	PERCENTAGE CHANGE SINCE 03/22/04
DATA TRANSMISSION						
BYTE THROUGHPUT / MIN	4623.78	4835.73	7947.66	-3323.88	-1661.94	-41.82
BYTES SENT / MIN	3271.80	3196.69	6409.20	-3137.40	-1568.70	-48.95
BYTES RECEIVED / MIN	1351.98	1639.04	1538.46	-186.48	-93.24	-12.12
MESSAGE THROUGHPUT / MIN	9.67	973.65	736.37	-726.70	-363.35	-98.69
MESSAGES SENT / MIN	6.52	487.19	369.39	-362.87	-181.43	-98.23
MESSAGES RECEIVED / MIN	3.14	486.46	366.97	-363.83	-181.92	-99.14
TOTAL BYTES TRANSMITTED	2,635,776	2,611,292	4,291,762	-1,655,986	-827993.00	-38.59
BYTES SENT	1,865,084	1,726,213	3,460,989	-1,595,905	-797952.50	-46.11
BYTES RECEIVED	770,692	885,079	830,773	-60,081	-30040.50	-7.23
TOTAL MESSAGES TRANSMITTED	5,510	525,772	397,640	-392,130	-196065.00	-98.61
MESSAGES SENT	3,718	263,083	199,473	-195,755	-97877.50	-98.14
MESSAGES RECEIVED	1,792	262,689	198,167	-196,375	-98187.50	-99.10
POLLING DATA						
AVERAGE POLLING RATE / MIN	213.08	257.92	230.18	-17.10	-8.55	-7.43
AVERAGE WAIT FOR POLL (SECS)	0.00	0.00	0.00	0.00	0.00	8.03
PERCENT POSITIVE POLLS	1.38	1.15	3.14	-1.75	-0.88	-55.96
TOTAL POLL COUNT	121,464	139,278	124,296	-2,832	-1416.00	-2.28
POSITIVE POLL COUNT	1,677	1,597	3,897	-2,220	-1110.00	-56.97
ERROR DATA						
RETRANSMISSION PERCENTAGE	1.87	0.04	0.04	1.83	0.92	4695.61
NUMBER OF MESSAGES PER ERROR	21.19	2.68	2.02	19.17	9.59	947.93
ERROR COUNT	260	196,402	196,628	-196,368	-98184.00	-99.87
RETRANSMISSION COUNT	103	223	155	-52	-26.00	-33.55
UTILIZATION DATA						
PERCENT LINK UTILIZATION	3.21	3.36	5.52	-2.31	-1.15	-41.82
LINK SPEED (BITS/SECOND)	19,200	19,200	19,200	0	0.00	0.00

Figure 3-18A. NetSpy NCP Utilization by Link (Trend)

3.1.3.2.5 NLDM Workload by Application (SNT211)

INTENDED USAGE:

Use this display to quantify the workload volume a given host application imposes on the network. You can monitor this report for indications that the maximum supportable utilization level is being reached.

FORMAT:

This display indicates the character and path information unit (PIU) data for selected primary logical units (PLUs). You can see a sample display of the profile report in Figure 3-19.

DATABASE FILE: SNTLSY

DATA ELEMENTS USED:

NETWRKID	SYSID	PLU	ZONE	LSYNRCBR	LSYNRCBS
LSYNRTBS	LSYNRTBR	LSYNRCPR	LSYNRCPS	LSYNRTPS	LSYNRTPR
LSYTRESC					

CALCULATIONS:

$$\text{PER\_MIN} = (\text{ENDTS} - \text{STARTTS}) / 60$$

$$\text{TOTAL CONTROL BYTES} / \text{MIN} = \text{SUM}(\text{LSYNRCBR}, \text{LSYNRCBS})$$

$$\text{CONTROL BYTES SENT} / \text{MIN} = \text{LSYNRCBS} / \text{PER\_MIN}$$

$$\text{CONTROL BYTES RECEIVED} / \text{MIN} = \text{LSYNRCBR} / \text{PER\_MIN}$$

$$\text{TOTAL TEXT BYTES} / \text{MIN} = \text{SUM}(\text{LSYNRTBS}, \text{LSYNRTBR})$$

$$\text{TEXT BYTES SENT} / \text{MIN} = \text{LSYNRTBS} / \text{PER\_MIN}$$

$$\text{TEXT BYTES RECEIVED} / \text{MIN} = \text{LSYNRTBR} / \text{PER\_MIN}$$

$$\text{TOTAL BYTES} / \text{MIN} = \text{SUM}(\text{LSYNRCBR}, \text{LSYNRCBS}, \text{LSYNRTBS}, \text{LSYNRTBR}) / \text{PER\_MIN}$$

$$\text{TOTAL BYTES SENT} / \text{MIN} = \text{SUM}(\text{LSYNRCBS}, \text{LSYNRTBS}) / \text{PER\_MIN}$$

TOTAL BYTES RECEIVED / MIN = SUM(LSYNRCBR,LSYNRTBR)

TOTAL CONTROL PIUS / MIN = SUM(LSYNRCPR,LSYNRCPS)

CONTROL PIUS SENT / MIN = LSYNRCPS / PER_MIN

CONTROL PIUS RECEIVED / MIN = LSYNRCPR / PER_MIN

TOTAL TEXT PIUS / MIN = SUM(LSYNRTPS,LSYNRTPR)

TEXT PIUS SENT / MIN = LSYNRTPS / PER_MIN

TEXT PIUS RECEIVED / MIN = LSYNRTPR / PER_MIN

TOTAL PIUS / MIN = SUM(LSYNRCPR,LSYNRCPS,LSYNRTPS,LSYNRTPR)
/ PER_MIN

TOTAL PIUS SENT / MIN = SUM(LSYNRCPS,LSYNRTPS) / PER_MIN

TOTAL PIUS RECEIVED / MIN = SUM(LSYNRCPR,LSYNRTPR)
/ PER_MIN

TOTAL BYTES TRANSMITTED =
SUM(LSYNRTBR,LSYNRTBS,LSYNRCBR,LSYNRCBS)

CONTROL BYTES TRANSMITTED = SUM(LSYNRCBR,LSYNRCBS)

TEXT BYTES TRANSMITTED = SUM(LSYNRTBR,LSYNRTBS)

TOTAL PIUS TRANSMITTED =
SUM(LSYNRTPR,LSYNRTPS,LSYNRCPR,LSYNRCPS)

CONTROL PIUS TRANSMITTED = SUM(LSYNRCPR,LSYNRCPS)

TEXT PIUS TRANSMITTED = SUM(LSYNRTPR,LSYNRTPS)

AVERAGE BYTES PER CONTROL PIU SENT = LSYNRCBS / LSYNRCPS

AVERAGE BYTES PER CONTROL PIU REC'D = LSYNRCBR / LSYNRCPR

AVERAGE BYTES PER TEXT PIU SENT = LSYNRTBS / LSYNRTPS

AVERAGE BYTES PER TEXT PIU REC'D = LSYNRTBR / LSYNRTPR

USAGE CONSIDERATIONS:

You can vary the number of PLUs for which reports are produced by changing the value of the %SL211 macro in

prefix.MICS.USER.SOURCE(#SNTRPTS). The default macro
selects all PLUs.

CA MICS NETWORK COMPONENT
(SNT211) NLDM WORKLOAD BY APPLICATION: IMSPROD
NETWORK: NETWORK1 SYSTEM: TS02
PRODUCED: AUGUST 7, 2003 ZONE: PRIME TIME

+-----+-----+	
ACTIVITY INDICATORS	08/05/03
+-----+-----+	
THROUGHPUT DATA	
TOTAL CONTROL BYTES / MIN	21.58
CTRL BYTES SENT / MIN	19.72
CTRL BYTES RECEIVED / MIN	1.86
TOTAL TEXT BYTES / MIN	59,305.68
TEXT BYTES SENT / MIN	47,082.80
TEXT BYTES RECEIVED / MIN	12,222.88
TOTAL BYTES / MIN	59,327.26
TOTAL BYTES SENT / MIN	47,102.52
TOTAL BYTES RECEIVED / MIN	12,224.74
TOTAL CTRL PIUS / MIN	45.86
CTRL PIUS SENT / MIN	1.62
CTRL PIUS RECEIVED / MIN	44.24
TOTAL TEXT PIUS / MIN	106.77
TEXT PIUS SENT / MIN	40.79
TEXT PIUS RECEIVED / MIN	65.98
TOTAL PIUS / MIN	152.62
TOTAL PIUS SENT / MIN	42.41
TOTAL PIUS RECEIVED / MIN	110.22
WORKLOAD STATISTICS	
TOTAL BYTES TRANSMITTED	717,391,673
CTRL BYTES TRANSMITTED	260,907
TEXT BYTES TRANSMITTED	717,130,766
TOTAL PIUS TRANSMITTED	1,845,528
CTRL PIUS TRANSMITTED	554,496
TEXT PIUS TRANSMITTED	1,291,032
TOTAL RESPONSES	23
AVG BYTES PER CNTL PIU SENT	12.18
AVG BYTES PER CNTL PIU REC'D	0.04
AVG BYTES PER TEXT PIU SENT	1154.35
AVG BYTES PER TEXT PIU REC'D	185.25

+-----+

Figure 3-19. NLDM Workload by Application (Profile)

3.1.3.2.6 NLDM Workload by Link (SNT212)

INTENDED USAGE:

Use this display to quantify the workload volume for each monitored network link. You can monitor this report for indications that the maximum supportable utilization level is being reached.

FORMAT:

This display indicates the character and path information unit (PIU) throughput for selected links. You can see a sample display of the profile report in Figure 3-20.

DATABASE FILE: NVSNLL

DATA ELEMENTS USED:

NETWRKID	SYSID	SLULINK	ZONE	NLLNRCBR	NLLNRCBS
NLLNRTBS	NLLNRTBR	NLLNRCPR	NLLNRCPS	NLLNRTPS	NLLNRTPR
NLLTRES					

CALCULATIONS:

$$\text{PER\_MIN} = (\text{ENDTS} - \text{STARTTS}) / 60$$
$$\text{TOTAL CONTROL BYTES} / \text{MIN} = \text{SUM}(\text{NLLNRCBR}, \text{NLLNRCBS})$$
$$\text{CONTROL BYTES SENT} / \text{MIN} = \text{NLLNRCBS} / \text{PER\_MIN}$$
$$\text{CONTROL BYTES RECEIVED} / \text{MIN} = \text{NLLNRCBR} / \text{PER\_MIN}$$
$$\text{TOTAL TEXT BYTES} / \text{MIN} = \text{SUM}(\text{NLLNRTBS}, \text{NLLNRTBR})$$
$$\text{TEXT BYTES SENT} / \text{MIN} = \text{NLLNRTBS} / \text{PER\_MIN}$$
$$\text{TEXT BYTES RECEIVED} / \text{MIN} = \text{NLLNRTBR} / \text{PER\_MIN}$$
$$\text{TOTAL BYTES} / \text{MIN} = \text{SUM}(\text{NLLNRCBR}, \text{NLLNRCBS}, \text{NLLNRTBS}, \text{NLLNRTBR}) / \text{PER\_MIN}$$
$$\text{TOTAL BYTES SENT} / \text{MIN} = \text{SUM}(\text{NLLNRCBS}, \text{NLLNRTBS}) / \text{PER\_MIN}$$
$$\text{TOTAL BYTES RECEIVED} / \text{MIN} = \text{SUM}(\text{NLLNRCBR}, \text{NLLNRTBR})$$

$$\text{TOTAL CONTROL PIUS} / \text{MIN} = \text{SUM}(\text{NLLNRCPR}, \text{NLLNRCPS})$$

$$\text{CONTROL PIUS SENT} / \text{MIN} = \text{NLLNRCPS} / \text{PER\_MIN}$$

$$\text{CONTROL PIUS RECEIVED} / \text{MIN} = \text{NLLNRCPR} / \text{PER\_MIN}$$

$$\text{TOTAL TEXT PIUS} / \text{MIN} = \text{SUM}(\text{NLLNRTPS}, \text{NLLNRTPR})$$

$$\text{TEXT PIUS SENT} / \text{MIN} = \text{NLLNRTPS} / \text{PER\_MIN}$$

$$\text{TEXT PIUS RECEIVED} / \text{MIN} = \text{NLLNRTPR} / \text{PER\_MIN}$$

$$\text{TOTAL PIUS} / \text{MIN} = \text{SUM}(\text{NLLNRCPR}, \text{NLLNRCPS}, \text{NLLNRTPS}, \text{NLLNRTPR}) / \text{PER\_MIN}$$

$$\text{TOTAL PIUS SENT} / \text{MIN} = \text{SUM}(\text{NLLNRCPS}, \text{NLLNRTPS}) / \text{PER\_MIN}$$

$$\text{TOTAL PIUS RECEIVED} / \text{MIN} = \text{SUM}(\text{NLLNRCPR}, \text{NLLNRTPR}) / \text{PER\_MIN}$$

$$\text{TOTAL BYTES TRANSMITTED} = \text{SUM}(\text{NLLNRTBR}, \text{NLLNRTBS}, \text{NLLNRCBR}, \text{NLLNRCBS})$$

$$\text{CONTROL BYTES TRANSMITTED} = \text{SUM}(\text{NLLNRCBR}, \text{NLLNRCBS})$$

$$\text{TEXT BYTES TRANSMITTED} = \text{SUM}(\text{NLLNRTBR}, \text{NLLNRTBS})$$

$$\text{TOTAL PIUS TRANSMITTED} = \text{SUM}(\text{NLLNRTPR}, \text{NLLNRTPS}, \text{NLLNRCPR}, \text{NLLNRCPS})$$

$$\text{CONTROL PIUS TRANSMITTED} = \text{SUM}(\text{NLLNRCPR}, \text{NLLNRCPS})$$

$$\text{TEXT PIUS TRANSMITTED} = \text{SUM}(\text{NLLNRTPR}, \text{NLLNRTPS})$$

$$\text{AVERAGE BYTES PER CONTROL PIU SENT} = \text{NLLNRCBS} / \text{NLLNRCPS}$$

$$\text{AVERAGE BYTES PER CONTROL PIU REC'D} = \text{NLLNRCBR} / \text{NLLNRCPR}$$

$$\text{AVERAGE BYTES PER TEXT PIU SENT} = \text{NLLNRTBS} / \text{NLLNRTPS}$$

$$\text{AVERAGE BYTES PER TEXT PIU REC'D} = \text{NLLNRTBR} / \text{NLLNRTPR}$$

USAGE CONSIDERATIONS:

You can vary the number of links for which reports are produced by changing the value of the %SL212 macro in prefix.MICS.USER.SOURCE(#SNTRPTS). The default macro

selects all links.

CA MICS NETWORK COMPONENT
 (SNT212) NLDM WORKLOAD BY LINK: L1032
 NETWORK: NETWORK1 SYSTEM: TS02
 PRODUCED: AUGUST 7, 2003 ZONE: PRIME TIME

+-----+	
ACTIVITY INDICATORS	08/05/03
+-----+	
THROUGHPUT DATA	
TOTAL CONTROL BYTES / MIN	0.39
CTRL BYTES SENT / MIN	0.21
CTRL BYTES RECEIVED / MIN	0.18
TOTAL TEXT BYTES / MIN	805.20
TEXT BYTES SENT / MIN	549.03
TEXT BYTES RECEIVED / MIN	256.17
TOTAL BYTES / MIN	805.59
TOTAL BYTES SENT / MIN	549.24
TOTAL BYTES RECEIVED / MIN	256.35
TOTAL CTRL PIUS / MIN	0.32
CTRL PIUS SENT / MIN	0.03
CTRL PIUS RECEIVED / MIN	0.29
TOTAL TEXT PIUS / MIN	1.74
TEXT PIUS SENT / MIN	0.47
TEXT PIUS RECEIVED / MIN	1.27
TOTAL PIUS / MIN	2.06
TOTAL PIUS SENT / MIN	0.50
TOTAL PIUS RECEIVED / MIN	1.56
WORKLOAD STATISTICS	
TOTAL BYTES TRANSMITTED	9,243,551
CTRL BYTES TRANSMITTED	4,446
TEXT BYTES TRANSMITTED	9,239,105
TOTAL PIUS TRANSMITTED	23,588
CTRL PIUS TRANSMITTED	3,660
TEXT PIUS TRANSMITTED	19,928
TOTAL RESPONSES	
AVG BYTES PER CNTL PIU SENT	7.16
AVG BYTES PER CNTL PIU REC'D	0.62
AVG BYTES PER TEXT PIU SENT	1177.08
AVG BYTES PER TEXT PIU REC'D	201.66

+-----+

Figure 3-20. NLDM Workload by Link (Profile)

3.1.3.2.7 NLDM Workload by Control Unit (SNT213)

INTENDED USAGE:

Use this display to quantify the workload volume for each monitored terminal controller (physical unit). You can monitor this report for indications that the maximum supportable utilization level is being reached.

The job that produces this display will not execute or will cause unpredictable results unless both the value and the label for account code SNTACT3 is set to SLUPU for NetView/NLDM or CA NetMaster data. For information on how to define account codes, see Section 7.2.

FORMAT:

This display indicates the character and path information unit (PIU) throughput of selected control units. You can see a sample display of the profile report in Figure 3-21.

DATABASE FILE: NVNSA

DATA ELEMENTS USED:

NETWRKID	SYSID	SLULINK	ZONE	NSANRCBR	NSANRCBS
NSANRTBS	NSANRTBR	NSANRCPR	NSANRCPS	NSANRTPS	NSANRTPR
NSATRESC					

CALCULATIONS:

$$\text{PER\_MIN} = (\text{ENDTS} - \text{STARTTS}) / 60$$

$$\text{TOTAL CONTROL BYTES} / \text{MIN} = \text{SUM}(\text{NSANRCBR}, \text{NSANRCBS})$$

$$\text{CONTROL BYTES SENT} / \text{MIN} = \text{NSANRCBS} / \text{PER\_MIN}$$

$$\text{CONTROL BYTES RECEIVED} / \text{MIN} = \text{NSANRCBR} / \text{PER\_MIN}$$

$$\text{TOTAL TEXT BYTES} / \text{MIN} = \text{SUM}(\text{NSANRTBS}, \text{NSANRTBR})$$

$$\text{TEXT BYTES SENT} / \text{MIN} = \text{NSANRTBS} / \text{PER\_MIN}$$

$$\text{TEXT BYTES RECEIVED} / \text{MIN} = \text{NSANRTBR} / \text{PER\_MIN}$$

TOTAL BYTES / MIN = SUM(NSANRCBR, NSANRCBS, NSANRTBS, NSANRTBR)
/ PER_MIN

TOTAL BYTES SENT / MIN = SUM(NSANRCBS, NSANRTBS) / PER_MIN

TOTAL BYTES RECEIVED / MIN = SUM(NSANRCBR, NSANRTBR)

TOTAL CONTROL PIUS / MIN = SUM(NSANRCPR, NSANRCPS)

CONTROL PIUS SENT / MIN = NSANRCPS / PER_MIN

CONTROL PIUS RECEIVED / MIN = NSANRCPR / PER_MIN

TOTAL TEXT PIUS / MIN = SUM(NSANRTPS, NSANRTPR)

TEXT PIUS SENT / MIN = NSANRTPS / PER_MIN

TEXT PIUS RECEIVED / MIN = NSANRTPR / PER_MIN

TOTAL PIUS / MIN = SUM(NSANRCPR, NSANRCPS, NSANRTPS, NSANRTPR)
/ PER_MIN

TOTAL PIUS SENT / MIN = SUM(NSANRCPS, NSANRTPS) / PER_MIN

TOTAL PIUS RECEIVED / MIN = SUM(NSANRCPR, NSANRTPR)
/ PER_MIN

TOTAL BYTES TRANSMITTED =
SUM(NSANRTBR, NSANRTBS, NSANRCBR, NSANRCBS)

CONTROL BYTES TRANSMITTED = SUM(NSANRCBR, NSANRCBS)

TEXT BYTES TRANSMITTED = SUM(NSANRTBR, NSANRTBS)

TOTAL PIUS TRANSMITTED =
SUM(NSANRTPR, NSANRTPS, NSANRCPR, NSANRCPS)

CONTROL PIUS TRANSMITTED = SUM(NSANRCPR, NSANRCPS)

TEXT PIUS TRANSMITTED = SUM(NSANRTPR, NSANRTPS)

AVERAGE BYTES PER CONTROL PIU SENT = NSANRCBS / NSANRCPS

AVERAGE BYTES PER CONTROL PIU REC'D = NSANRCBR / NSANRCPR

AVERAGE BYTES PER TEXT PIU SENT = NSANRTBS / NSANRTPS

AVERAGE BYTES PER TEXT PIU REC'D = NSANRTBR / NSANRTPR

USAGE CONSIDERATIONS:

You can report on various number of control units by changing the value of the %SL213 macro in prefix.MICS.USER.SOURCE(#SNTRPTS). The default macro selects all control units.

CA MICS NETWORK COMPONENT
(SNT213) NLDM WORKLOAD BY CONTROL UNIT (SLUPU): P09972
NETWORK: NETWORK1 SYSTEM: TS02
PRODUCED: AUGUST 7, 2003 ZONE: PRIME TIME

+-----+	
ACTIVITY INDICATORS	08/01/03
+-----+	
THROUGHPUT DATA	
TOTAL CONTROL BYTES / MIN	1.38
CTRL BYTES SENT / MIN	0.96
CTRL BYTES RECEIVED / MIN	0.42
TOTAL TEXT BYTES / MIN	518.00
TEXT BYTES SENT / MIN	421.36
TEXT BYTES RECEIVED / MIN	96.64
TOTAL BYTES / MIN	519.38
TOTAL BYTES SENT / MIN	422.32
TOTAL BYTES RECEIVED / MIN	97.06
TOTAL CTRL PIUS / MIN	0.69
CTRL PIUS SENT / MIN	0.18
CTRL PIUS RECEIVED / MIN	0.52
TOTAL TEXT PIUS / MIN	1.59
TEXT PIUS SENT / MIN	0.73
TEXT PIUS RECEIVED / MIN	0.85
TOTAL PIUS / MIN	2.28
TOTAL PIUS SENT / MIN	0.91
TOTAL PIUS RECEIVED / MIN	1.37
WORKLOAD STATISTICS	
TOTAL BYTES TRANSMITTED	5,355,218
CTRL BYTES TRANSMITTED	14,206
TEXT BYTES TRANSMITTED	5,341,012
TOTAL PIUS TRANSMITTED	23,532
CTRL PIUS TRANSMITTED	7,164
TEXT PIUS TRANSMITTED	16,368
AVG BYTES PER CNTL PIU SENT	5.38
AVG BYTES PER CNTL PIU REC'D	0.81
AVG BYTES PER TEXT PIU SENT	574.99
AVG BYTES PER TEXT PIU REC'D	113.07

+-----+

Figure 3-21. NLDM Workload by Control Unit (Profile)

3.1.3.2.8 NLDM Workload by Terminal (SNT214)

INTENDED USAGE:

Use this display to quantify the workload volume imposed on the network by the devices attached to a given terminal. You can monitor this report for indications that the maximum supportable utilization level of the terminal is being reached.

FORMAT:

This display indicates the character and path information unit (PIU) throughput for selected terminals. You can see a sample display of the profile report in Figure 3-22.

DATABASE FILE: NVNSA

DATA ELEMENTS USED:

NETWRKID	SYSID	SLULINK	ZONE	NSANRCBR	NSANRCBS
NSANRTBS	NSANRTBR	NSANRCPR	NSANRCPS	NSANRTPS	NSANRTPR
NSATRESC					

CALCULATIONS:

$$\text{PER\_MIN} = (\text{ENDTS} - \text{STARTTS}) / 60$$
$$\text{TOTAL CONTROL BYTES} / \text{MIN} = \text{SUM}(\text{NSANRCBR}, \text{NSANRCBS})$$
$$\text{CONTROL BYTES SENT} / \text{MIN} = \text{NSANRCBS} / \text{PER\_MIN}$$
$$\text{CONTROL BYTES RECEIVED} / \text{MIN} = \text{NSANRCBR} / \text{PER\_MIN}$$
$$\text{TOTAL TEXT BYTES} / \text{MIN} = \text{SUM}(\text{NSANRTBS}, \text{NSANRTBR})$$
$$\text{TEXT BYTES SENT} / \text{MIN} = \text{NSANRTBS} / \text{PER\_MIN}$$
$$\text{TEXT BYTES RECEIVED} / \text{MIN} = \text{NSANRTBR} / \text{PER\_MIN}$$
$$\text{TOTAL BYTES} / \text{MIN} = \text{SUM}(\text{NSANRCBR}, \text{NSANRCBS}, \text{NSANRTBS}, \text{NSANRTBR}) / \text{PER\_MIN}$$
$$\text{TOTAL BYTES SENT} / \text{MIN} = \text{SUM}(\text{NSANRCBS}, \text{NSANRTBS}) / \text{PER\_MIN}$$

TOTAL BYTES RECEIVED / MIN = SUM(NSANRCBR,NSANRTBR)

TOTAL CONTROL PIUS / MIN = SUM(NSANRCPR,NSANRCPS)

CONTROL PIUS SENT / MIN = NSANRCPS / PER_MIN

CONTROL PIUS RECEIVED / MIN = NSANRCPR / PER_MIN

TOTAL TEXT PIUS / MIN = SUM(NSANRTPS,NSANRTPR)

TEXT PIUS SENT / MIN = NSANRTPS / PER_MIN

TEXT PIUS RECEIVED / MIN = NSANRTPR / PER_MIN

TOTAL PIUS / MIN = SUM(NSANRCPR,NSANRCPS,NSANRTPS,NSANRTPR)
/ PER_MIN

TOTAL PIUS SENT / MIN = SUM(NSANRCPS,NSANRTPS) / PER_MIN

TOTAL PIUS RECEIVED / MIN = SUM(NSANRCPR,NSANRTPR)
/ PER_MIN

TOTAL BYTES TRANSMITTED =
SUM(NSANRTBR,NSANRTBS,NSANRCBR,NSANRCBS)

CONTROL BYTES TRANSMITTED = SUM(NSANRCBR,NSANRCBS)

TEXT BYTES TRANSMITTED = SUM(NSANRTBR,NSANRTBS)

TOTAL PIUS TRANSMITTED =
SUM(NSANRTPR,NSANRTPS,NSANRCPR,NSANRCPS)

CONTROL PIUS TRANSMITTED = SUM(NSANRCPR,NSANRCPS)

TEXT PIUS TRANSMITTED = SUM(NSANRTPR,NSANRTPS)

AVERAGE BYTES PER CONTROL PIU SENT = NSANRCBS / NSANRCPS

AVERAGE BYTES PER CONTROL PIU REC'D = NSANRCBR / NSANRCPR

AVERAGE BYTES PER TEXT PIU SENT = NSANRTBS / NSANRTPS

AVERAGE BYTES PER TEXT PIU REC'D = NSANRTBR / NSANRTPR

USAGE CONSIDERATIONS:

You can report on a different number of terminals by
changing the value of the %SL214 macro in

prefix.MICS.USER.SOURCE(#SNTRPTS). The default macro selects all SLUs.

CA MICS NETWORK COMPONENT
 (SNT214) NLDM WORKLOAD BY TERMINAL (SLU) : VTAA9
 NETWORK: NETWORK1 SYSTEM: TS02
 PRODUCED: AUGUST 7, 2003 ZONE: WEEKENDS

+-----+	
ACTIVITY INDICATORS	08/05/03
+-----+	
THROUGHPUT DATA	
TOTAL CONTROL BYTES / MIN	0.09
CTRL BYTES SENT / MIN	0.08
CTRL BYTES RECEIVED / MIN	0.01
TOTAL TEXT BYTES / MIN	149.84
TEXT BYTES SENT / MIN	148.35
TEXT BYTES RECEIVED / MIN	1.49
TOTAL BYTES / MIN	149.92
TOTAL BYTES SENT / MIN	148.42
TOTAL BYTES RECEIVED / MIN	1.50
TOTAL CTRL PIUS / MIN	0.03
CTRL PIUS SENT / MIN	0.01
CTRL PIUS RECEIVED / MIN	0.01
TOTAL TEXT PIUS / MIN	0.37
TEXT PIUS SENT / MIN	0.19
TEXT PIUS RECEIVED / MIN	0.18
TOTAL PIUS / MIN	0.39
TOTAL PIUS SENT / MIN	0.20
TOTAL PIUS RECEIVED / MIN	0.19
WORKLOAD STATISTICS	
TOTAL BYTES TRANSMITTED	173,085
CTRL BYTES TRANSMITTED	103
TEXT BYTES TRANSMITTED	172,982
TOTAL PIUS TRANSMITTED	456
CTRL PIUS TRANSMITTED	30
TEXT PIUS TRANSMITTED	426
AVG BYTES PER CNTL PIU SENT	5.75
AVG BYTES PER CNTL PIU REC'D	0.79
AVG BYTES PER TEXT PIU SENT	792.88
AVG BYTES PER TEXT PIU REC'D	8.19
+-----+	

Figure 3-22. NLDM Workload by Terminal (Profile)

3.1.3.2.9 NPM/NetSpy NCP Utilization by Link (SNT215)

SOURCE:

The source for this report can be either Tivoli NetView NPM Network data or CA NetSpy NCP interface data.

INTENDED USAGE:

Use this display to identify and quantify potential network link over-utilization conditions.

FORMAT:

This display indicates the workload and utilization of selected links supported by each NCP. The report header will also identify the type of link data based upon the DATATYPE element. You can see sample displays of profile and trend reports in these figures:

- o 3-23 3-23A (NPM NTRI Physical Link)
- o 3-23B 3-23C (NPM NTRI Logical Link)
- o 3-23D 3-23E (NPM X.25 Link)
- o 3-24 3-24A (CA NetSpy NTRI Physical Link)
- o 3-24B 3-24C (CA NetSpy NTRI Logical Link)

DATABASE FILE: SNTNCL

DATA ELEMENTS USED:

NETNAME	ZONE	NCLNRPIU	NCLPCLBS	LINKSPD	DATATYPE
NCLPMCHS	NCLPMCHR	NCLPMSS	NCLPMSR	NCLNRCHS	NCLNRCHR
NCLNMSS	NCLNRMSR	NCLPMTPL	NCLNRTPPL	NCLNRPL	NCLNRERR

CALCULATIONS:

BYTE THROUGHPUT / MIN =

$$\text{SUM}(\text{NCLNRCHR}, \text{NCLNRCHS}) / \text{DURATION} / 60$$

MESSAGE THROUGHPUT / MIN = $\text{SUM}(\text{NCLNRMSR}, \text{NCLNRMSS})$

TOTAL BYTES TRANSMITTED = $\text{SUM}(\text{NCLNRCHR}, \text{NCLNRCHS})$

TOTAL MESSAGES TRANSMITTED = $\text{SUM}(\text{NCLNRMSS}, \text{NCLNRMSR})$

AVERAGE WAIT FOR POLL (SECS) =
 $((\text{DURATION} / 60) / \text{NCLNRTPL}) / 2$

PERCENT POSITIVE POLLS = $(\text{NCLNRPPL} / \text{NCLNRTPL}) * 100$

RETRANSMISSION PERCENTAGE =
 $(\text{NCLNRPIU} / \text{SUM}(\text{NCLNRMSS}, \text{NCLNRMSR})) * 100$

NUMBER OF MESSAGES PER ERROR =
 $\text{SUM}(\text{NCLNRMSS}, \text{NCLNRMSR}) / \text{NCLNRERR}$

PERCENT LINK UTILIZATION =
 $((\text{NCLNRCHR} + \text{NCLNRCHS}) / (\text{NCLNRRLS} / 10)) * (\text{ENDTS} - \text{STARTTS})) * 100$

USAGE CONSIDERATIONS:

You can report on different number of links by changing the value of the %SL215 macro in prefix.MICS.USER.SOURCE(#SNTRPTS). The default macro selects all links.

CA MICS NETWORK COMPONENT

(SNT215) NPM LINK UTILIZATION FOR NTRI-P LINK: RINGLNE

NETWORK: NETWORK1 SYSTEM: S002
 PRODUCED: APRIL 4, 2004 ZONE: PRIME TIME

ACTIVITY INDICATORS	03/30/04
DATA TRANSMISSION	
BYTE THROUGHPUT / MIN	15154.53
BYTES SENT / MIN	12573.46
BYTES RECEIVED / MIN	2581.06
I-FRAMES THROUGHPUT / MIN	84.61
I-FRAMES SENT / MIN	52.83
I-FRAMES RECEIVED / MIN	31.78
TOTAL BYTES TRANSMITTED	5,228,312
BYTES SENT	4,337,845
BYTES RECEIVED	890,467
TOTAL I-FRAMES TRANSMITTED	29,191
I-FRAMES SENT	18,227
I-FRAMES RECEIVED	10,964
POLLING DATA (X25 ONLY)	
RECEIVER READY (SEND)	
RECEIVER READY (RECEIVE)	
RECEIVER NOT READY (SEND)	
RECEIVER NOT READY (RECEIVE)	
ERROR DATA	
I-FRAME RETRANSMISSION %	0.00
I-FRAME RETRANSMISSION COUN	0
BYTES-RETRANSMISSION %	0.00
BYTES RETRANSMISSION COUNT	0
UTILIZATION DATA	
COMBINED LINK UTILIZATION %	0.09
LINK UTILIZATION % (SEND)	17.46
LINK SPEED (SEND)	9,600
LINK UTILIZATION % (RECEIVE)	3.58
LINK SPEED (RECEIVE)	9,600

Figure 3-23. NPM NCP Utilization by Link (Profile)

CA MICS NETWORK COMPONENT						
(SNT215) NPM LINK UTILIZATION FOR NTRI-P LINK: RINGLNE						
NETWORK: NETWORK1 SYSTEM: S002						
PRODUCED: APRIL 4, 2004 ZONE: PRIME TIME						
ACTIVITY INDICATORS	03/30/04	03/29/04		AMOUNT OF CHANGE SINCE	PER-PERIOD RATE OF CHANGE SINCE	PERCENTAGE CHANGE SINCE
DATA TRANSMISSION						
BYTE THROUGHPUT / MIN	15154.53	10753.80				
BYTES SENT / MIN	12573.46	8925.01				
BYTES RECEIVED / MIN	2581.06	1828.79				
I-FRAMES THROUGHPUT / MIN	84.61	59.43				
I-FRAMES SENT / MIN	52.83	37.06				
I-FRAMES RECEIVED / MIN	31.78	22.37				
TOTAL BYTES TRANSMITTED	5,228,312	1,129,149				
BYTES SENT	4,337,845	937,126				
BYTES RECEIVED	890,467	192,023				
TOTAL I-FRAMES TRANSMITTED	29,191	6,240				
I-FRAMES SENT	18,227	3,891				
I-FRAMES RECEIVED	10,964	2,349				
POLLING DATA (X25 ONLY)						
RECEIVER READY (SEND)						
RECEIVER READY (RECEIVE)						
RECEIVER NOT READY (SEND)						
RECEIVER NOT READY (RECEIVE)						
ERROR DATA						
I-FRAME RETRANSMISSION %	0.00	0.00				
I-FRAME RETRANSMISSION COUN	0	0				
BYTES-RETRANSMISSION %	0.00	0.00				
BYTES RETRANSMISSION COUNT	0	0				
UTILIZATION DATA						
COMBINED LINK UTILIZATION %	0.09	0.06				
LINK UTILIZATION % (SEND)	17.46	12.40				
LINK SPEED (SEND)	9,600	9,600				
LINK UTILIZATION % (RECEIVE)	3.58	2.54				
LINK SPEED (RECEIVE)	9,600	9,600				

Figure 3-23A. NPM NCP Utilization by Link (Trend)

CA MICS NETWORK COMPONENT

(SNT215) NPM LINK UTILIZATION FOR NTRI-L LINK: J000N009

NETWORK: NETWORK1 SYSTEM: S002
 PRODUCED: APRIL 4, 2004 ZONE: PRIME TIME

ACTIVITY INDICATORS	03/30/04
DATA TRANSMISSION	
BYTE THROUGHPUT / MIN	15153.71
BYTES SENT / MIN	12573.46
BYTES RECEIVED / MIN	2580.25
I-FRAMES THROUGHPUT / MIN	84.61
I-FRAMES SENT / MIN	52.83
I-FRAMES RECEIVED / MIN	31.78
TOTAL BYTES TRANSMITTED	5,228,030
BYTES SENT	4,337,845
BYTES RECEIVED	890,185
TOTAL I-FRAMES TRANSMITTED	29,191
I-FRAMES SENT	18,227
I-FRAMES RECEIVED	10,964
POLLING DATA (X25 ONLY)	
RECEIVER READY (SEND)	
RECEIVER READY (RECEIVE)	
RECEIVER NOT READY (SEND)	
RECEIVER NOT READY (RECEIVE)	
ERROR DATA	
I-FRAME RETRANSMISSION %	0.00
I-FRAME RETRANSMISSION COUNT	0
BYTES-RETRANSMISSION %	0.00
BYTES RETRANSMISSION COUNT	0
UTILIZATION DATA	
COMBINED LINK UTILIZATION %	
LINK UTILIZATION % (SEND)	
LINK SPEED (SEND)	
LINK UTILIZATION % (RECEIVE)	
LINK SPEED (RECEIVE)	

Figure 3-23B. NPM NCP Utilization by Link (Profile)

CA MICS NETWORK COMPONENT						
(SNT215) NPM LINK UTILIZATION FOR NTRI-L LINK: J000N009						
NETWORK: NETWORK1 SYSTEM: S002						
PRODUCED: APRIL 4, 2004 ZONE: PRIME TIME						
ACTIVITY INDICATORS	03/30/04	03/29/04		AMOUNT OF CHANGE SINCE	PER-PERIOD RATE OF CHANGE SINCE	PERCENTAGE CHANGE SINCE
DATA TRANSMISSION						
BYTE THROUGHPUT / MIN	15153.71	10753.80				
BYTES SENT / MIN	12573.46	8925.01				
BYTES RECEIVED / MIN	2580.25	1828.79				
I-FRAMES THROUGHPUT / MIN	84.61	59.43				
I-FRAMES SENT / MIN	52.83	37.06				
I-FRAMES RECEIVED / MIN	31.78	22.37				
TOTAL BYTES TRANSMITTED	5,228,030	1,129,149				
BYTES SENT	4,337,845	937,126				
BYTES RECEIVED	890,185	192,023				
TOTAL I-FRAMES TRANSMITTED	29,191	6,240				
I-FRAMES SENT	18,227	3,891				
I-FRAMES RECEIVED	10,964	2,349				
POLLING DATA (X25 ONLY)						
RECEIVER READY (SEND)						
RECEIVER READY (RECEIVE)						
RECEIVER NOT READY (SEND)						
RECEIVER NOT READY (RECEIVE)						
ERROR DATA						
I-FRAME RETRANSMISSION %	0.00	0.00				
I-FRAME RETRANSMISSION COUN	0	0				
BYTES-RETRANSMISSION %	0.00	0.00				
BYTES RETRANSMISSION COUNT	0	0				
UTILIZATION DATA						
COMBINED LINK UTILIZATION %						
LINK UTILIZATION % (SEND)						
LINK SPEED (SEND)						
LINK UTILIZATION % (RECEIVE)						
LINK SPEED (RECEIVE)						

Figure 3-23C. NPM NCP Utilization by Link (Trend)

CA MICS NETWORK COMPONENT

(SNT215) NPM LINK UTILIZATION FOR X25- LINK: XM23070

NETWORK: NETWORK1 SYSTEM: S002

PRODUCED: APRIL 4, 2004 ZONE: PRIME TIME

ACTIVITY INDICATORS	03/30/04
DATA TRANSMISSION	
BYTE THROUGHPUT / MIN	17314.25
BYTES SENT / MIN	12892.54
BYTES RECEIVED / MIN	4421.71
I-FRAMES THROUGHPUT / MIN	577.22
I-FRAMES SENT / MIN	274.35
I-FRAMES RECEIVED / MIN	302.88
TOTAL BYTES TRANSMITTED	5,973,416
BYTES SENT	4,447,926
BYTES RECEIVED	1,525,490
TOTAL I-FRAMES TRANSMITTED	199,142
I-FRAMES SENT	94,650
I-FRAMES RECEIVED	104,492
POLLING DATA (X25 ONLY)	
RECEIVER READY (SEND)	28,981
RECEIVER READY (RECEIVE)	70,297
RECEIVER NOT READY (SEND)	0
RECEIVER NOT READY (RECEIVE)	0
ERROR DATA	
I-FRAME RETRANSMISSION %	0.00
I-FRAME RETRANSMISSION COUNT	0
BYTES-RETRANSMISSION %	0.00
BYTES RETRANSMISSION COUNT	0
UTILIZATION DATA	
COMBINED LINK UTILIZATION %	12.02
LINK UTILIZATION % (SEND)	17.91
LINK SPEED (SEND)	9,600
LINK UTILIZATION % (RECEIVE)	6.14
LINK SPEED (RECEIVE)	9,600

Figure 3-23D. NPM NCP Utilization by Link (Profile)

CA MICS NETWORK COMPONENT						
(SNT215) NPM LINK UTILIZATION FOR X25- LINK: XM23070						
NETWORK: NETWORK1 SYSTEM: S002						
PRODUCED: APRIL 4, 2004 ZONE: PRIME TIME						
ACTIVITY INDICATORS	03/30/04	03/29/04		AMOUNT OF CHANGE SINCE	PER-PERIOD RATE OF CHANGE SINCE	PERCENTAGE CHANGE SINCE
DATA TRANSMISSION						
BYTE THROUGHPUT / MIN	17314.25	14781.59				
BYTES SENT / MIN	12892.54	9214.97				
BYTES RECEIVED / MIN	4421.71	5566.62				
I-FRAMES THROUGHPUT / MIN	577.22	457.28				
I-FRAMES SENT / MIN	274.35	224.76				
I-FRAMES RECEIVED / MIN	302.88	232.51				
TOTAL BYTES TRANSMITTED	5,973,416	1,552,067				
BYTES SENT	4,447,926	967,572				
BYTES RECEIVED	1,525,490	584,495				
TOTAL I-FRAMES TRANSMITTED	199,142	48,014				
I-FRAMES SENT	94,650	23,600				
I-FRAMES RECEIVED	104,492	24,414				
POLLING DATA (X25 ONLY)						
RECEIVER READY (SEND)	28,981	7,724				
RECEIVER READY (RECEIVE)	70,297	18,115				
RECEIVER NOT READY (SEND)	0	0				
RECEIVER NOT READY (RECEIVE)	0	0				
ERROR DATA						
I-FRAME RETRANSMISSION %	0.00	0.00				
I-FRAME RETRANSMISSION COUN	0	0				
BYTES-RETRANSMISSION %	0.00	0.00				
BYTES RETRANSMISSION COUNT	0	0				
UTILIZATION DATA						
COMBINED LINK UTILIZATION %	12.02	10.26				
LINK UTILIZATION % (SEND)	17.91	12.80				
LINK SPEED (SEND)	9,600	9,600				
LINK UTILIZATION % (RECEIVE)	6.14	7.73				
LINK SPEED (RECEIVE)	9,600	9,600				

Figure 3-23E. NPM NCP Utilization by Link (Trend)

CA MICS NETWORK COMPONENT

(SNT215) NETSPY LINK UTILIZATION FOR NTRI-P LINK: L051088

NETWORK: NETWORK1 SYSTEM: S002
 PRODUCED: APRIL 4, 2004 ZONE: NON PRIME

+-----+	
ACTIVITY INDICATORS	03/24/04
+-----+	
DATA TRANSMISSION	
BYTE THROUGHPUT / MIN	59516.47
BYTES SENT / MIN	46314.59
BYTES RECEIVED / MIN	13201.88
I-FRAMES THROUGHPUT / MIN	201.77
I-FRAMES SENT / MIN	118.85
I-FRAMES RECEIVED / MIN	82.92
TOTAL BYTES TRANSMITTED	12,541,112
BYTES SENT	9,759,256
BYTES RECEIVED	2,781,856
TOTAL I-FRAMES TRANSMITTED	42,517
I-FRAMES SENT	25,044
I-FRAMES RECEIVED	17,473
POLLING DATA (X25 ONLY)	
RECEIVER READY (SEND)	
RECEIVER READY (RECEIVE)	
RECEIVER NOT READY (SEND)	
RECEIVER NOT READY (RECEIVE)	
ERROR DATA	
I-FRAME RETRANSMISSION %	0.32
I-FRAME RETRANSMISSION COUN	134
BYTES-RETRANSMISSION %	0.32
BYTES RETRANSMISSION COUNT	40,413
UTILIZATION DATA	
COMBINED LINK UTILIZATION %	1.08
LINK UTILIZATION % (SEND)	
LINK SPEED (SEND)	0
LINK UTILIZATION % (RECEIVE)	
LINK SPEED (RECEIVE)	0
+-----+	

Figure 3-24. NetSpy NCP Utilization by Link (Profile)

CA MICS NETWORK COMPONENT						
(SNT215) NETSPY LINK UTILIZATION FOR NTRI-P LINK: L051088						
NETWORK: NETWORK1 SYSTEM: S002						
PRODUCED: APRIL 4, 2004 ZONE: NON PRIME						
ACTIVITY INDICATORS	03/24/04	03/23/04	03/22/04	AMOUNT OF CHANGE SINCE 03/22/04	PER-PERIOD RATE OF CHANGE SINCE 03/22/04	PERCENTAGE CHANGE SINCE 03/22/04
DATA TRANSMISSION						
BYTE THROUGHPUT / MIN	59516.47	94664.21	214404.20	-154887.73	-77443.87	-72.24
BYTES SENT / MIN	46314.59	75247.89	162297.14	-115982.55	-57991.27	-71.46
BYTES RECEIVED / MIN	13201.88	19416.32	52107.06	-38905.18	-19452.59	-74.66
I-FRAMES THROUGHPUT / MIN	201.77	337.41	749.30	-547.53	-273.76	-73.07
I-FRAMES SENT / MIN	118.85	199.66	427.04	-308.19	-154.09	-72.17
I-FRAMES RECEIVED / MIN	82.92	137.75	322.26	-239.34	-119.67	-74.27
TOTAL BYTES TRANSMITTED	12,541,112	22,787,254	80,555,232	-68,014,120	-34007060.00	-84.43
BYTES SENT	9,759,256	18,113,421	60,977,740	-51,218,484	-25609242.00	-84.00
BYTES RECEIVED	2,781,856	4,673,833	19,577,492	-16,795,636	-8397818.00	-85.79
TOTAL I-FRAMES TRANSMITTED	42,517	81,220	281,525	-239,008	-119504.00	-84.90
I-FRAMES SENT	25,044	48,061	160,446	-135,402	-67701.00	-84.39
I-FRAMES RECEIVED	17,473	33,159	121,079	-103,606	-51803.00	-85.57
POLLING DATA (X25 ONLY)						
RECEIVER READY (SEND)						
RECEIVER READY (RECEIVE)						
RECEIVER NOT READY (SEND)						
RECEIVER NOT READY (RECEIVE)						
ERROR DATA						
I-FRAME RETRANSMISSION %	0.32	0.59	0.91	-0.59	-0.30	-65.34
I-FRAME RETRANSMISSION COUN	134	481	2,560	-2,426	-1213.00	-94.77
BYTES-RETRANSMISSION %	0.32	0.71	1.07	-0.75	-0.38	-70.01
BYTES RETRANSMISSION COUNT	40,413	161,167	865,470	-825,057	-412528.50	-95.33
UTILIZATION DATA						
COMBINED LINK UTILIZATION %	1.08	1.64	3.35	-2.27	-1.14	-67.84
LINK UTILIZATION % (SEND)						
LINK SPEED (SEND)	0	0	0	0	0.00	
LINK UTILIZATION % (RECEIVE)						
LINK SPEED (RECEIVE)	0	0	0	0	0.00	

Figure 3-24A. NetSpy NCP Utilization by Link (Trend)

CA MICS NETWORK COMPONENT

(SNT215) NETSPY LINK UTILIZATION FOR NTRI-L LINK: L051088B

NETWORK: NETWORK1 SYSTEM: S002
 PRODUCED: APRIL 4, 2004 ZONE: NON PRIME

+-----+	
ACTIVITY INDICATORS	03/24/04
-----+	
DATA TRANSMISSION	
BYTE THROUGHPUT / MIN	4573.00
BYTES SENT / MIN	3118.72
BYTES RECEIVED / MIN	1454.28
I-FRAMES THROUGHPUT / MIN	17.56
I-FRAMES SENT / MIN	8.90
I-FRAMES RECEIVED / MIN	8.66
TOTAL BYTES TRANSMITTED	963,608
BYTES SENT	657,167
BYTES RECEIVED	306,441
TOTAL I-FRAMES TRANSMITTED	3,701
I-FRAMES SENT	1,876
I-FRAMES RECEIVED	1,825
POLLING DATA (X25 ONLY)	
RECEIVER READY (SEND)	
RECEIVER READY (RECEIVE)	
RECEIVER NOT READY (SEND)	
RECEIVER NOT READY (RECEIVE)	
ERROR DATA	
I-FRAME RETRANSMISSION %	0.22
I-FRAME RETRANSMISSION COUN	8
BYTES-RETRANSMISSION %	0.29
BYTES RETRANSMISSION COUNT	2,800
UTILIZATION DATA	
COMBINED LINK UTILIZATION %	
LINK UTILIZATION % (SEND)	
LINK SPEED (SEND)	
LINK UTILIZATION % (RECEIVE)	
LINK SPEED (RECEIVE)	
+-----+	

Figure 3-24B. NetSpy NCP Utilization by Link (Profile)

CA MICS NETWORK COMPONENT						
(SNT215) NETSPY LINK UTILIZATION FOR NTRI-L LINK: L051088B						
NETWORK: NETWORK1 SYSTEM: S002						
PRODUCED: APRIL 4, 2004 ZONE: NON PRIME						
ACTIVITY INDICATORS	03/24/04	03/23/04	03/22/04	AMOUNT OF CHANGE SINCE 03/22/04	PER-PERIOD RATE OF CHANGE SINCE 03/22/04	PERCENTAGE CHANGE SINCE 03/22/04
DATA TRANSMISSION						
BYTE THROUGHPUT / MIN	4573.00	7537.31	3371.50	1201.51	600.75	35.64
BYTES SENT / MIN	3118.72	5118.93	1961.54	1157.19	578.59	58.99
BYTES RECEIVED / MIN	1454.28	2418.38	1409.96	44.32	22.16	3.14
I-FRAMES THROUGHPUT / MIN	17.56	27.73	17.23	0.34	0.17	1.96
I-FRAMES SENT / MIN	8.90	15.09	8.79	0.11	0.06	1.27
I-FRAMES RECEIVED / MIN	8.66	12.64	8.43	0.23	0.11	2.68
TOTAL BYTES TRANSMITTED	963,608	1,814,356	1,266,727	-303,119	-151559.50	-23.93
BYTES SENT	657,167	1,232,212	736,982	-79,815	-39907.50	-10.83
BYTES RECEIVED	306,441	582,144	529,745	-223,304	-111652.00	-42.15
TOTAL I-FRAMES TRANSMITTED	3,701	6,676	6,472	-2,771	-1385.50	-42.82
I-FRAMES SENT	1,876	3,633	3,303	-1,427	-713.50	-43.20
I-FRAMES RECEIVED	1,825	3,043	3,169	-1,344	-672.00	-42.41
POLLING DATA (X25 ONLY)						
RECEIVER READY (SEND)						
RECEIVER READY (RECEIVE)						
RECEIVER NOT READY (SEND)						
RECEIVER NOT READY (RECEIVE)						
ERROR DATA						
I-FRAME RETRANSMISSION %	0.22	0.25	0.14	0.08	0.04	55.44
I-FRAME RETRANSMISSION COUNT	8	17	9	-1	-0.50	-11.11
BYTES-RETRANSMISSION %	0.29	0.48	0.06	0.23	0.12	382.41
BYTES RETRANSMISSION COUNT	2,800	8,775	763	2,037	1018.50	266.97
UTILIZATION DATA						
COMBINED LINK UTILIZATION %						
LINK UTILIZATION % (SEND)						
LINK SPEED (SEND)						
LINK UTILIZATION % (RECEIVE)						
LINK SPEED (RECEIVE)						

Figure 3-24C. NetSpy NCP Utilization by Link (Trend)

3.1.3.2.10 NPM/NetSpy NCP Utilization by Link (SNT216)

SOURCE:

The source for this report can be either Tivoli NPM Network data or CA NetSpy NCP interface data.

INTENDED USAGE:

Use this display to identify and quantify potential network link over-utilization conditions.

FORMAT:

This display indicates the workload and utilization of selected links supported by each NCP. The report header also identifies the type of link data based on the DATATYPE element. You can see sample displays of profile and trend reports in these figures:

- o 3-25 (NPM TIC3 Physical Link)
- o 3-26 (CA NetSpy TIC3 Physical Link)

DATABASE FILE: SNTNCL

DATA ELEMENTS USED:

NETNAME	ZONE	NCLPCLBS	LINKSPD	DATATYPE	NCLNRRBY
NCLPMCHS	NCLPMCHR	NCLPMIFS	NCLPMIFR	NCLNRCHS	NCLNRCHR
NCLNRIFS	NCLNRIFR	NCLPNRRFD	NCLNRRFM	NCLNRRFU	NCLNRRIF
SYSID					

CALCULATIONS:

BYTE THROUGHPUT / MIN =

$$\text{SUM}(\text{NCLNRCHR}, \text{NCLNRCHS}) / \text{DURATION} / 60$$

I-FRAME THROUGHPUT / MIN = $\text{SUM}(\text{NCLNRIFR}, \text{NCLNRIFS})$

TOTAL BYTES TRANSMITTED = $\text{SUM}(\text{NCLNRCHR}, \text{NCLNRCHS})$

TOTAL I-FRAMES TRANSMITTED = $\text{SUM}(\text{NCLNRIFR}, \text{NCLNRIFS})$

RETRANSMISSION PERCENTAGE =

$$(NCLNRRIF / \text{SUM}(NCLNRIFR, NCLNRIFS)) * 100$$

PERCENT LINK UTILIZATION =
$$((NCLNRCHR + NCLNRCHS) / (NCLNRRLS / 10)) * (ENDTS - STARTTS) * 100$$

USAGE CONSIDERATIONS:

You can report on a different number of links by changing the value of the %SL216 macro in prefix.MICS.USER.SOURCE(#SNTRPTS). The default macro selects all links.

CA MICS NETWORK COMPONENT

(SNT216) NPM LINK UTILIZATION FOR TIC3-P LINK: L21TD2

NETWORK: NETWORK1 SYSTEM: SSPA
 PRODUCED: OCTOBER 14, 2004 ZONE: PRIME TIME

ACTIVITY INDICATORS	01/11/04
DATA TRANSMISSION	
BYTE THROUGHPUT / MIN	2173204.58
BYTES SENT / MIN	1663623.34
BYTES RECEIVED / MIN	509581.23
I-FRAMES THROUGHPUT / MIN	7995.35
I-FRAMES SENT / MIN	3678.81
I-FRAMES RECEIVED / MIN	4316.54
TOTAL BYTES TRANSMITTED	391,176,824
BYTES SENT	299,452,202
BYTES RECEIVED	91,724,622
TOTAL I-FRAMES TRANSMITTED	1,439,163
I-FRAMES SENT	662,185
I-FRAMES RECEIVED	776,978
MISCELLANEOUS DATA	
DISCARDED FRAMES	0
MISADDRESSED FRAMES RECEIVED	0
UNRECOGNIZED FRAMES	26
ERROR DATA	
I-FRMS RETRANSMISSION %	0.02
I-FRMS RETRANSMISSION COUNT	356
BYTES RETRANSMISSION %	0.02
BYTES RETRANSMISSION COUNT	80,343
UTILIZATION DATA	
COMBINED LINK UTILIZATION %	1.81
LINK UTILIZATION % (SEND)	1.39
LINK SPEED (SEND)	16,000,000
LINK UTILIZATION % (RECEIVE)	0.42
LINK SPEED (RECEIVE)	16,000,000

Figure 3-25. NPM NCP Utilization by Link (Profile)

CA MICS NETWORK COMPONENT (SNT216) NPM LINK UTILIZATION FOR TIC3-P LINK: L21TD2 NETWORK: NETWORK1 SYSTEM: SSPA PRODUCED: OCTOBER 14, 2004 ZONE: PRIME TIME						
ACTIVITY INDICATORS	01/11/04	.	.	AMOUNT OF CHANGE SINCE	PER-PERIOD RATE OF CHANGE SINCE	PERCENTAGE CHANGE SINCE
DATA TRANSMISSION						
BYTE THROUGHPUT / MIN	2173204.58					
BYTES SENT / MIN	1663623.34					
BYTES RECEIVED / MIN	509581.23					
I-FRAMES THROUGHPUT / MIN	7995.35					
I-FRAMES SENT / MIN	3678.81					
I-FRAMES RECEIVED / MIN	4316.54					
TOTAL BYTES TRANSMITTED	391,176,824					
BYTES SENT	299,452,202					
BYTES RECEIVED	91,724,622					
TOTAL I-FRAMES TRANSMITTED	1,439,163					
I-FRAMES SENT	662,185					
I-FRAMES RECEIVED	776,978					
MISCELLANEOUS DATA						
DISCARDED FRAMES	0					
MISADDRESSED FRAMES RECEIVED	0					
UNRECOGNIZED FRAMES	26					
ERROR DATA						
I-FRMS RETRANSMISSION %	0.02					
I-FRMS RETRANSMISSION COUNT	356					
BYTES RETRANSMISSION %	0.02					
BYTES RETRANSMISSION COUNT	80,343					
UTILIZATION DATA						
COMBINED LINK UTILIZATION %	1.81					
LINK UTILIZATION % (SEND)	1.39					
LINK SPEED (SEND)	16,000,000					
LINK UTILIZATION % (RECEIVE)	0.42					
LINK SPEED (RECEIVE)	16,000,000					

Figure 3-26. NPM NCP Utilization by Link (Trend)

3.1.3.2.11 NetSpy Workload by Application (SNT221)

INTENDED USAGE:

Use this display to quantify the workload volume a given host application imposes on the network. Monitor this report for indications that the maximum supportable utilization level is being reached.

FORMAT:

This display indicates the character traffic for selected primary logical units (PLUs). You can see a sample display of the profile report in Figure 3-27.

DATABASE FILE: SNTNSP

DATA ELEMENTS USED:

NETWRKID	SYSID	PLU	ZONE	NSPTRESC
NSPNRBYS	NSPNRBYR			

CALCULATIONS:

$$\text{PERMIN} = (\text{ENDTS} - \text{STARTTS}) / 60$$

$$\text{TOTAL RESPONSES} = \text{NSPTRESC}$$

$$\text{TOTAL BYTES} = \text{SUM}(\text{NSPNRBYR}, \text{NSPNRBYS})$$

$$\text{TOTAL BYTES SENT} = \text{NSPNRBYS}$$

$$\text{TOTAL BYTES RECEIVED} = \text{NSPNRBYR}$$

$$\text{TOTAL BYTES} / \text{MIN} = \text{SUM}(\text{NSPNRBYR}, \text{NSPNRBYS}) / \text{PERMIN}$$

$$\text{TOTAL BYTES SENT} / \text{MIN} = \text{NSPNRBYS} / \text{PERMIN}$$

$$\text{TOTAL BYTES RECEIVED} / \text{MIN} = \text{NSPNRBYR} / \text{PERMIN}$$

$$\text{NUMBER OF RESPONSES} / \text{MIN} = \text{NSPTRESC} / \text{PERMIN}$$

$$\text{AVERAGE BYTES PER RESPONSE SENT} = \text{NSPNRBYS} / \text{NSPTRESC}$$

$$\text{AVERAGE BYTES PER RESPONSE REC'D} = \text{NSPNRBYR} / \text{NSPTRESC}$$

USAGE CONSIDERATIONS:

You can report on a different number of PLUs by changing the value of the %SL221 macro in prefix.MICS.USER.SOURCE(#SNTRPTS). The default macro selects all PLUs.

CA MICS NETWORK COMPONENT

(SNT221) NETSPY WORKLOAD BY APPLICATION: CICS

NETWORK: NETWORK1 SYSTEM: SYSA
PRODUCED: JANUARY 21, 2004 ZONE: PRIME TIME

+-----+		
	ACTIVITY INDICATORS	01/20/04
+-----+		
	WORKLOAD STATISTICS	
	TOTAL RESPONSES	312,067
	TOTAL BYTES	418,819,570
	TOTAL BYTES SENT	381,547,446
	TOTAL BYTES RECEIVED	37,272,124
	TOTAL BYTES / MIN	218,818
	TOTAL BYTES SENT / MIN	199,345
	TOTAL BYTES RECEIVED / MIN	19,473
	NUMBER OF RESPONSES / MIN	163
	AVG BYTES PER RESPONSE SENT	1,223
	AVG BYTES PER RESPONSE REC'D	119
+-----+		

Figure 3-27. NetSpy Workload by Application (Profile)

3.1.3.2.12 NetSpy Workload by Terminal (SNT222)

INTENDED USAGE:

Use this display to quantify the workload volume that individual terminals impose on the network. Monitor this report for indications that a terminal may be monopolizing a terminal controller or communications line.

FORMAT:

This display indicates character traffic for selected terminals. The report header will also identify the type of application session data based upon the NSSLU62F flag element. You can see sample displays of profile and trend reports in these figures:

- o 3-28 3-28A (LU6.2 Profile/Trend Reports)
- o 3-28B 3-28C (NON-LU6.2 Profile/Trend Reports)

DATABASE FILE: SNTNSS

DATA ELEMENTS USED:

NETWRKID	SYSID	ZONE	NSSNRBYR	NSSNRBYS
NSSTRESC	NSSLU62F	NSSNRURM	NSSNRTRI	

CALCULATIONS:

$$\text{PERMIN} = (\text{ENDTS} - \text{STARTTS}) / 60$$

$$\text{TOTAL RESPONSES} = \text{NSSTRESC}$$

$$\text{TOTAL BYTES} = \text{SUM}(\text{NSSNRBYR}, \text{NSSNRBYS})$$

$$\text{TOTAL BYTES SENT} = \text{NSSNRBYS}$$

$$\text{TOTAL BYTES RECEIVED} = \text{NSSNRBYR}$$

$$\text{TOTAL BYTES} / \text{MIN} = \text{SUM}(\text{NSSNRBYR}, \text{NSSNRBYS}) / \text{PERMIN}$$

$$\text{TOTAL BYTES SENT} / \text{MIN} = \text{NSSNRBYS} / \text{PERMIN}$$

$$\text{TOTAL BYTES RECEIVED} / \text{MIN} = \text{NSSNRBYR} / \text{PERMIN}$$

NUMBER OF RESPONSES / MIN = NSSTRESC / PERMIN

AVERAGE BYTES PER RESPONSE SENT = NSSNRBYS / NSSTRESC

AVERAGE BYTES PER RESPONSE REC'D = NSSNRBYR / NSSTRESC

USAGE CONSIDERATIONS:

You can vary the number of terminals for which reports are produced by changing the value of the %SL222 macro in prefix.MICS.USER.SOURCE(#SNTRPTS). The default macro selects all SLUs.

CA MICS NETWORK COMPONENT
 (SNT222) NETSPY WORKLOAD FOR TERMINAL: LU27004X LU62SES=Y

NETWORK: NETWORK1 SYSTEM: NSRA
 PRODUCED: OCTOBER 14, 2004 ZONE: PRIME TIME

ACTIVITY INDICATORS	08/22/04
WORKLOAD STATISTICS	
TOTAL NO. OF RESPONSES	1
TOTAL NO. OF NETWORK RESPONSE	1
TOTAL NO. OF USER RESPONSES	1
TOTAL LU62 TRANSACTIONS INITS	1
TOTAL BYTES	
TOTAL BYTES SENT	74,176
TOTAL BYTES RECEIVED	710
TOTAL BYTES / MIN	14,977.20
TOTAL BYTES SENT / MIN	14,835.20
TOTAL BYTES RECEIVED / MIN	142.00
NUMBER OF RESPONSES / MIN	0.20
AVG BYTES PER RESPONSE SENT	74,176.00
AVG BYTES PER RESPONSE REC'D	710.00

Figure 2-28. NetSpy Workload by Terminal (Profile)

CA MICS NETWORK COMPONENT (SNT222) NETSPY WORKLOAD FOR TERMINAL: LU27004X LU62SES=Y NETWORK: NETWORK1 SYSTEM: NSRA PRODUCED: OCTOBER 14, 2004 ZONE: PRIME TIME						
ACTIVITY INDICATORS	08/22/04	.	.	AMOUNT OF CHANGE SINCE	PER-PERIOD RATE OF CHANGE SINCE	PERCENTAGE CHANGE SINCE
WORKLOAD STATISTICS						
TOTAL NO. OF RESPONSES	1					
TOTAL NO. OF NETWORK RESPONSE	1					
TOTAL NO. OF USER RESPONSES	1					
TOTAL LU62 TRANSACTIONS INITS	1					
TOTAL BYTES						
TOTAL BYTES SENT	74,176					
TOTAL BYTES RECEIVED	710					
TOTAL BYTES / MIN	14,977.20					
TOTAL BYTES SENT / MIN	14,835.20					
TOTAL BYTES RECEIVED / MIN	142.00					
NUMBER OF RESPONSES / MIN	0.20					
AVG BYTES PER RESPONSE SENT	74,176.00					
AVG BYTES PER RESPONSE REC'D	710.00					

Figure 2-28A. NetSpy Workload by Terminal (Trend)

CA MICS NETWORK COMPONENT
 (SNT222) NETSPY WORKLOAD FOR TERMINAL: TPPG002 LU62SES=N

NETWORK: NETWORK1 SYSTEM: NSRA
 PRODUCED: OCTOBER 14, 2004 ZONE: PRIME TIME

ACTIVITY INDICATORS		08/22/04
WORKLOAD STATISTICS		
TOTAL NO. OF RESPONSES		65
TOTAL NO. OF NETWORK RESPONSE		56
TOTAL NO. OF USER RESPONSES		56
TOTAL LU62 TRANSACTIONS INITS		0
TOTAL BYTES		
TOTAL BYTES SENT		553,882
TOTAL BYTES RECEIVED		930
TOTAL BYTES / MIN		6,164.58
TOTAL BYTES SENT / MIN		6,154.24
TOTAL BYTES RECEIVED / MIN		10.33
NUMBER OF RESPONSES / MIN		0.72
AVG BYTES PER RESPONSE SENT		8,521.26
AVG BYTES PER RESPONSE REC'D		14.31

Figure 2-28B. NetSpy Workload by Terminal (Profile)

3.1 Tabular Reports

CA MICS NETWORK COMPONENT (SNT222) NETSPY WORKLOAD FOR TERMINAL: TPPG002 LU62SES=N NETWORK: NETWORK1 SYSTEM: NSRA PRODUCED: OCTOBER 14, 2004 ZONE: PRIME TIME						
ACTIVITY INDICATORS	08/22/04	.	.	AMOUNT OF CHANGE SINCE	PER-PERIOD RATE OF CHANGE SINCE	PERCENTAGE CHANGE SINCE
WORKLOAD STATISTICS						
TOTAL NO. OF RESPONSES	65					
TOTAL NO. OF NETWORK RESPONSE	56					
TOTAL NO. OF USER RESPONSES	56					
TOTAL LU62 TRANSACTIONS INITS	0					
TOTAL BYTES	0					
TOTAL BYTES SENT	553,882					
TOTAL BYTES RECEIVED	930					
TOTAL BYTES / MIN	6,164.58					
TOTAL BYTES SENT / MIN	6,154.24					
TOTAL BYTES RECEIVED / MIN	10.33					
NUMBER OF RESPONSES / MIN	0.72					
AVG BYTES PER RESPONSE SENT	8,521.26					
AVG BYTES PER RESPONSE REC'D	14.31					

Figure 2-28C. NetSpy Workload by Terminal (Trend)

3.1.3.3 CA MICS Class 3 Reports

These reports are not supported in the current release of the CA MICS Network Analyzer.

3.1.3.4 Data Collection Reports

Data collection reports indicate whether data was being collected for specific network components during a measurement period. The NPM/NetSpy NCP data collection report is produced using either Tivoli NetView NPM network data or CA NetSpy NCP interface data. The NPM session data collection report is produced using Tivoli NetView NPM session data. Both reports can be produced either in profile format, displaying data retained in a single cycle of the CA MICS database or in trend format, comparing three cycles of data from the database.

The data collection reports are explained in greater detail in the following sections:

- 1 - NPM/NetSpy NCP Link Data Collection (SNT401)
- 2 - NPM Session Data Collection (SNT403)

3.1.3.4.1 NPM/NetSpy NCP Link Data Collection (SNT401)

SOURCE:

The source for this report can be either Tivoli NetView NPM Network data or CA NetSpy NCP interface data.

INTENDED USAGE:

Use this display to identify the network resources for which Netview NPM network data or CA NetSpy NCP interface data was collected. Conclusions you draw from measurement data are only valid if you consider the scope of that data. This display identifies the scope of either NetView NPM network data collection or CA NetSpy NCP interface data collection.

FORMAT:

This display indicates the timestamp of the first and last data records that the component processes for each network resource. In addition, the number of DETAIL records represented by the data is displayed along with the average number of DETAIL records per hour. You can see sample displays of profile and trend reports in Figures 3-29, 3-29A, and 3-30.

DATABASE FILE: SNTNCL

DATA ELEMENTS USED:

NETWRKID	NETNAME	INTERVLS	STARTTS	ENDTS

CALCULATIONS:

$$\text{DETAIL RECORDS COLLECTED, AVERAGE / HOUR} = \frac{\text{INTERVLS}}{((\text{ENDTS} - \text{STARTTS}) / 3600)}$$

USAGE CONSIDERATIONS:

We use data only from the SNTNCL File to produce this display. Thus, any recording of activity for any component on a link causes an entry for that link. Low values in the Records Collected columns may indicate

missing data and should be investigated further.

IMPORTANT: Although no data is recorded for intervals during which a given network component is inoperative, this display is not intended to indicate availability. You can report on a different number of links by changing the value of the %SL401 macro in prefix.MICS.USER.SOURCE(#SNTRPTS). The default macro selects all links.

CA MICS NETWORK COMPONENT					
(SNT401) NPM NCP LINK DATA COLLECTION STATISTICS					
NETWORK: NETWORK1 SYSTEM: 3084					
PRODUCED: OCTOBER 20, 2003 ZONE: PRIME TIME					
09/18/03	DATA COLLECTION TIMESTAMPS		DETAIL RECORDS COLLECTED		
	START	END	TOTAL	AVERAGE/HOUR	
LINK: ABLINK1	18SEP03:08:29:21	18SEP03:14:29:19	6	1.00	
LINK: ADLINK1	18SEP03:08:29:21	18SEP03:14:29:19	6	1.00	
LINK: ALLINK1	18SEP03:08:29:20	18SEP03:14:29:19	6	1.00	
LINK: ATLINK1	18SEP03:08:29:20	18SEP03:14:29:19	6	1.00	
LINK: CHLINK1	18SEP03:08:29:20	18SEP03:14:29:19	6	1.00	
LINK: DALINK1	18SEP03:08:29:20	18SEP03:14:29:19	6	1.00	
LINK: DVLINK1	18SEP03:08:29:20	18SEP03:14:29:19	6	1.00	
LINK: FCLINK1	18SEP03:08:29:20	18SEP03:14:29:19	6	1.00	
LINK: FCLINK2	18SEP03:08:29:20	18SEP03:14:29:19	6	1.00	
LINK: F2LINK1	18SEP03:08:29:20	18SEP03:14:29:19	6	1.00	
LINK: F2LINK2	18SEP03:08:29:20	18SEP03:14:29:19	6	1.00	
LINK: F2LINK3	18SEP03:08:29:20	18SEP03:14:29:19	6	1.00	
LINK: F2LINK4	18SEP03:08:29:20	18SEP03:14:29:19	6	1.00	
LINK: F3LINK1	18SEP03:08:29:20	18SEP03:14:29:19	6	1.00	
LINK: F3LINK2	18SEP03:08:29:20	18SEP03:14:29:19	6	1.00	
LINK: F4LINK1	18SEP03:08:29:20	18SEP03:14:29:19	6	1.00	
LINK: F5LINK1	18SEP03:08:29:21	18SEP03:14:29:19	6	1.00	
LINK: LALINK1	18SEP03:08:29:20	18SEP03:14:29:19	6	1.00	
LINK: LALINK2	18SEP03:08:29:20	18SEP03:14:29:19	6	1.00	
LINK: NASTECL	18SEP03:08:29:21	18SEP03:14:29:19	6	1.00	

Figure 3-29. NPM NCP Link Data Collection Statistics (Profile)

CA MICS NETWORK COMPONENT						
(SNT401) NPM NCP LINK DATA COLLECTION STATISTICS						
NETWORK: NETWORK1 SYSTEM: 3084						
PRODUCED: OCTOBER 20, 2003 ZONE: PRIME TIME						
09/18/03	09/17/03	09/16/03	DATA COLLECTION TIMESTAMPS		DETAIL RECORDS COLLECTED	
			START	END	TOTAL	AVERAGE/HOUR
LINK: ABLINK1	LINK: ABLINK1	LINK: ABLINK1	16SEP03:08:31:38	16SEP03:19:31:38	33	3.00
LINK: WALINK1	LINK: WALINK1	LINK: WALINK1	16SEP03:08:31:38	16SEP03:19:31:38	33	3.00
LINK: ALLINK1	LINK: ALLINK1	LINK: ALLINK1	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: ATLINK1	LINK: ATLINK1	LINK: ATLINK1	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: CHLINK1	LINK: CHLINK1	LINK: CHLINK1	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: DALINK1	LINK: DALINK1	LINK: DALINK1	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: DVLINK1	LINK: DVLINK1	LINK: DVLINK1	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: FCLINK1	LINK: FCLINK1	LINK: FCLINK1	16SEP03:08:31:38	16SEP03:19:31:37	33	3.00
LINK: FCLINK2	LINK: FCLINK2	LINK: FCLINK2	16SEP03:08:31:38	16SEP03:19:31:37	33	3.00
LINK: F2LINK1	LINK: F2LINK1	LINK: F2LINK1	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: F2LINK2	LINK: F2LINK2	LINK: F2LINK2	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: F2LINK3	LINK: F2LINK3	LINK: F2LINK3	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: F2LINK4	LINK: F2LINK4	LINK: F2LINK4	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: F3LINK1	LINK: F3LINK1	LINK: F3LINK1	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: F3LINK2	LINK: F3LINK2	LINK: F3LINK2	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: F4LINK1	LINK: F4LINK1	LINK: F4LINK1	16SEP03:08:31:38	16SEP03:19:31:38	33	3.00
LINK: F5LINK1	LINK: F5LINK1	LINK: F5LINK1	16SEP03:08:31:38	16SEP03:19:31:38	33	3.00
LINK: LALINK1	LINK: LALINK1	LINK: LALINK1	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00

Figure 3-29A. NPM NCP Link Data Collection Statistics (Trend)

CA MICS NETWORK COMPONENT						
(SNT401) NPM NCP LINK DATA COLLECTION STATISTICS						
NETWORK: NETWORK1 SYSTEM: 3084						
PRODUCED: OCTOBER 20, 2003 ZONE: PRIME TIME						
09/18/03	09/17/03	09/16/03	DATA COLLECTION TIMESTAMPS		DETAIL RECORDS COLLECTED	
			START	END	TOTAL	AVERAGE/HOUR
LINK: ABLINK1	LINK: ABLINK1	LINK: ABLINK1	16SEP03:08:31:38	16SEP03:19:31:38	33	3.00
LINK: WALINK1	LINK: WALINK1	LINK: WALINK1	16SEP03:08:31:38	16SEP03:19:31:38	33	3.00
LINK: ALLINK1	LINK: ALLINK1	LINK: ALLINK1	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: ATLINK1	LINK: ATLINK1	LINK: ATLINK1	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: CHLINK1	LINK: CHLINK1	LINK: CHLINK1	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: DALINK1	LINK: DALINK1	LINK: DALINK1	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: DVLINK1	LINK: DVLINK1	LINK: DVLINK1	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: FCLINK1	LINK: FCLINK1	LINK: FCLINK1	16SEP03:08:31:38	16SEP03:19:31:37	33	3.00
LINK: FCLINK2	LINK: FCLINK2	LINK: FCLINK2	16SEP03:08:31:38	16SEP03:19:31:37	33	3.00
LINK: F2LINK1	LINK: F2LINK1	LINK: F2LINK1	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: F2LINK2	LINK: F2LINK2	LINK: F2LINK2	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: F2LINK3	LINK: F2LINK3	LINK: F2LINK3	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: F2LINK4	LINK: F2LINK4	LINK: F2LINK4	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: F3LINK1	LINK: F3LINK1	LINK: F3LINK1	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: F3LINK2	LINK: F3LINK2	LINK: F3LINK2	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00
LINK: F4LINK1	LINK: F4LINK1	LINK: F4LINK1	16SEP03:08:31:38	16SEP03:19:31:38	33	3.00
LINK: F5LINK1	LINK: F5LINK1	LINK: F5LINK1	16SEP03:08:31:38	16SEP03:19:31:38	33	3.00
LINK: LALINK1	LINK: LALINK1	LINK: LALINK1	16SEP03:08:31:37	16SEP03:19:31:37	33	3.00

Figure 3-30. NetSpy NCP Link Data Collection Statistics (Profile)

3.1.3.4.2 NPM Session Data Collection (SNT403)

INTENDED USAGE:

This display identifies the network resources for the NPM session data that was collected. Conclusions you draw from measurement data are only valid if you consider the scope of that data. This display identifies the scope of NPM session data collection.

FORMAT:

This display indicates the timestamp of the first and last data records that were processed by the component for each network resource. In addition, the number of detail records represented by the data is displayed along with the average number of detail records per hour. You can see sample displays of profile and trend reports in figures 3-31 and 3-31A.

DATABASE FILE: SNTNPL

DATA ELEMENTS USED:

PLUSA, PLU, SLUSA, SLULINK, SLUPU, STARTTS, ENDTS, NETWRKID, INTERVLS

CALCULATIONS:

DETAIL RECORDS COLLECTED, AVERAGE / HOUR =
$$\text{INTERVLS} / ((\text{ENDTS} - \text{STARTTS}) / 3600)$$

USAGE CONSIDERATIONS:

Any recording of activity for a particular component causes an entry on the display. Low values in the Records Collected columns may indicate missing data and should be investigated further.

Note that, although no data is recorded for the intervals during which a given network component is inoperative, this display is not intended to indicate availability.

You can report on various numbers of links by changing the value of the %SL403 macro in member #SNTRPTS in prefix.MICS.USER.SOURCE. The default macro selects all links.

CA MICS NETWORK COMPONENT
(SNT403) NPM SESSION DATA COLLECTION STATISTICS
NETWORK: NETWORK1 SYSTEM: 3084
PRODUCED: AUGUST 01, 2003 ZONE: PRIME TIME

		DATA COLLECTION TIME STAMPS		DETAIL RECORDS COLLECTED	
07/01/03		START	END	TOTAL	AVERAGE/HOUR
LINK: SFLINK1					
PU: P3274264		01JUL03:14:01:15	01JUL03:18:31:15	259	57.56
PU: P3274265		01JUL03:14:00:15	01JUL03:18:35:46	303	65.99
PU: P3274266		01JUL03:14:10:46	01JUL03:17:13:15	53	17.43

Figure 3-31. NPM Session Data Collection Statistics (Profile)

		DATA COLLECTION TIME STAMPS		DETAIL RECORDS COLLECTED	
07/01/03		START	END	TOTAL	AVERAGE/HOUR
LINK: SFLINK1					
PU: P3274264	PU: P3274264	01JUL03:06:52:15	01JUL03:09:59:46	836	267.50
PU: P3274265	PU: P3274265	01JUL03:06:41:46	01JUL03:09:59:46	779	236.06
PU: P3274266	PU: P3274266	01JUL03:06:52:15	01JUL03:09:46:15	236	81.38

Figure 3-31A. NPM Session Data Collection Statistics (Trend)

3.1.3.5 CA MICS Class 5 Reports

These reports are not supported in the current release of the CA MICS Network Analyzer.

3.1.3.6 Network Incident Reports

Network incident reports indicate the occurrence of error conditions during network operation. These reports are produced using data collected by Tivoli NetView Hardware Monitor, NPDA, or CA NetMaster NEWS. You can produce network incident reports in either profile format, displaying data retained in a single cycle of the CA MICS database, or in trend format, comparing three cycles of data from the database.

The Network incident reports are explained in greater detail in the following sections:

- 1 - NPDA Event Analysis (SNT601)
- 2 - NPDA Statistics Analysis (SNT602)

3.1.3.6.1 NPDA Event Analysis (SNT601)

INTENDED USAGE:

Use this display to identify the network resources for which NPDA logged a permanent failure. You can use this data planning requirements for network support personnel and in scheduling preventive maintenance.

FORMAT:

This display indicates the time of the error for the affected resource, the resource type, a description of the type of error encountered, the number of errors of this type which occurred, and the number of NPDA alerts which were posted. You can see sample displays of profile and trend reports in Figures 3-32 and 3-32A.

DATABASE FILE: SNTNEF

DATA ELEMENTS USED:

NETWRKID NEFFRNAM NEFFRTYP NEFGEVCC NEFSEVCC NEFNRLT
NEFNREVT

CALCULATIONS:

None

USAGE CONSIDERATIONS:

You can report on different the numbers and types of NPDA events by changing the value of the %SL601 macro in prefix.MICS.USER.SOURCE(#SNT601). The default macro selects all events.

CA MICS NETWORK COMPONENT					
(SNT601) NPDA EVENT ANALYSIS					
NETWORK: NETWORK1 SYSTEM: 3084					
PRODUCED: OCTOBER 20, 2003 ZONE: PRIME TIME					
+-----+-----+-----+-----+-----+-----+					
RESOURCE		INCIDENT DESCRIPTION		10/17/03	
NAME	TYPE			INCIDENTS	ALERTS
+-----+-----+-----+-----+-----+-----+					
FCXA1	CTRL	SNA DATA STREAM ERROR:HOST PROGRAM		1	0
F2XA1	CTRL	SNA DATA STREAM ERROR:HOST PROGRAM		3	0
F2XA2	CTRL	SNA DATA STREAM ERROR:HOST PROGRAM		1	0
F3XA4	CTRL	SNA DATA STREAM ERROR:HOST PROGRAM		1	0
LAXA2	CTRL	DEVICE ERROR:DEVICE		5	0
LAXA3	CTRL	COAXIAL THRESHOLD:COAXIAL		3	0
PU32741	LCTL	CUSTOMIZATION ERROR:USER		1	0
RXAXA7	CTRL	DEVICE ERROR:DEVICE		4	0
RXBXA3	CTRL	SNA DATA STREAM ERROR:HOST PROGRAM		4	0
RXBXA5	CTRL	DEVICE ERROR:DEVICE		2	0
+-----+-----+-----+-----+-----+-----+					

Figure 3-32. NPDA Event Analysis (Profile)

CA MICS NETWORK COMPONENT									
(SNT601) NPDA EVENT ANALYSIS									
NETWORK: NETWORK1 SYSTEM: 3084									
PRODUCED: OCTOBER 20, 2003 ZONE: PRIME TIME									
RESOURCE		INCIDENT DESCRIPTION	10/17/03		10/16/03		10/15/03		
NAME	TYPE		INCIDENTS	ALERTS	INCIDENTS	ALERTS	INCIDENTS	ALERTS	
ARXA1	CTRL	DATA STREAM ERROR:HOST PROGRAM			1	0	2	0	
CHXA1	CTRL	DATA STREAM ERROR:HOST PROGRAM			1	0	2	0	
FCXA1	CTRL	DATA STREAM ERROR:HOST PROGRAM	1	0			2	0	
F2XA1	CTRL	DATA STREAM ERROR:HOST PROGRAM	3	0	2	0	4	0	
F2XA2	CTRL	DATA STREAM ERROR:HOST PROGRAM	1	0	1	0	3	0	
F3XA4	CTRL	DATA STREAM ERROR:HOST PROGRAM	1	0	1	0			
LAXA2	CTRL	DEVICE ERROR:DEVICE	5	0					
LAXA3	CTRL	COAXIAL THRESHOLD:COAXIAL	3	0	2	0	3	0	
PU227C0	LCTL	DEVICE ERROR:DEVICE			2	0			
PU32741	LCTL	DATA STREAM ERROR:HOST PROGRAM	1	0	1	0			
PU37771	CTRL	TIMEOUT:DEVICE OFF/REMOTE MODEM OFF/COMM			1	1	2	2	
RXAXA7	CTRL	DEVICE ERROR:DEVICE	4	0	10	0			
RXBXA1	CTRL	DATA STREAM ERROR:HOST PROGRAM			4	0			
RXBXA3	CTRL	DATA STREAM ERROR:HOST PROGRAM	4	0	2	0	2	0	
RXBXA5	CTRL	DATA STREAM ERROR:HOST PROGRAM	2	0	1	0	2	0	

Figure 3-32A. NPDA Event Analysis (Trend)

3.1.3.6.2 NPDA Statistics Analysis (SNT602)

INTENDED USAGE:

This display identifies the network resources for which Tivoli NetView Hardware Monitor NPDA logged temporary errors. Use this data in analyzing the cause of intermittent network performance degradation and in scheduling preventive maintenance for potentially failing devices.

FORMAT:

This display indicates the affected resource, the resource type, the number of temporary errors encountered, and the number of alerts which were posted. You can see sample displays of profile and trend reports in Figures 3-33 and 3-33A.

DATABASE FILE: SNTNSF

DATA ELEMENTS USED:

NETWRKID NSFFRNAM NSFFRTYP NSFTTERR NEFNRLT

CALCULATIONS:

None

USAGE CONSIDERATIONS:

You can vary the number and type of devices for which NPDA statistics are reported by changing the value of the %SL602 macro in prefix.MICS.USER.SOURCE(#SNTRPTS). The default macro selects all devices.

CA MICS NETWORK COMPONENT					
(SNT601) NPDA EVENT ANALYSIS					
NETWORK: NETWORK1 SYSTEM: 3084					
PRODUCED: OCTOBER 20, 2003 ZONE: PRIME TIME					
RESOURCE		INCIDENT DESCRIPTION	10/17/03		
NAME	TYPE		INCIDENTS	ALERTS	
FCXA1	CTRL	SNA DATA STREAM ERROR:HOST PROGRAM	1	0	
F2XA1	CTRL	SNA DATA STREAM ERROR:HOST PROGRAM	3	0	
F2XA2	CTRL	SNA DATA STREAM ERROR:HOST PROGRAM	1	0	
F3XA4	CTRL	SNA DATA STREAM ERROR:HOST PROGRAM	1	0	
LAXA2	CTRL	DEVICE ERROR:DEVICE	5	0	
LAXA3	CTRL	COAXIAL THRESHOLD:COAXIAL	3	0	
PU32741	LCTL	CUSTOMIZATION ERROR:USER	1	0	
RXAXA7	CTRL	DEVICE ERROR:DEVICE	4	0	
RXBXA3	CTRL	SNA DATA STREAM ERROR:HOST PROGRAM	4	0	
RXBXA5	CTRL	DEVICE ERROR:DEVICE	2	0	

Figure 3-33. NPDA Statistics Analysis (Profile)

CA MICS NETWORK COMPONENT									
(SNT602) NPDA STATISTICS ANALYSIS									
NETWORK: NETWORK1 SYSTEM: 3084									
PRODUCED: OCTOBER 20, 2003 ZONE: PRIME TIME									
RESOURCE			INCIDENT DESCRIPTION	10/10/03		10/09/03		10/08/03	
NAME	TYPE	INCIDENTS		ALERTS	INCIDENTS	ALERTS	INCIDENTS	ALERTS	
ARXA1	CTRL	TEMPORARY ERRORS			62	0			
ARXA2	CTRL	TEMPORARY ERRORS			45	0	63954	0	
ATXA1	CTRL	TEMPORARY ERRORS	85	2	1	0			
ATXA2	CTRL	TEMPORARY ERRORS			77	0			
CHXA1	CTRL	TEMPORARY ERRORS	58	0			64476	0	
CHXA2	CTRL	TEMPORARY ERRORS	33	0			63090	0	
DAXA1	CTRL	TEMPORARY ERRORS	67	0			65148	0	
DAXA2	CTRL	TEMPORARY ERRORS			75	0			
DDEVB2B	3380	TEMPORARY ERRORS			284	0			
DDEV120	3380	TEMPORARY ERRORS	344	0					
DDEV122	3380	TEMPORARY ERRORS	728	0					
DVXA1	CTRL	TEMPORARY ERRORS	123	0			65415	0	
DVXA2	CTRL	TEMPORARY ERRORS	2	0			65491	0	
FCXA1	CTRL	TEMPORARY ERRORS	88	0			59674	0	
FCXA2	CTRL	TEMPORARY ERRORS			31	0	61557	0	
FCXA3	CTRL	TEMPORARY ERRORS	111	0			65130	0	
F2XA1	CTRL	TEMPORARY ERRORS	34	0			57176	0	
F2XA2	CTRL	TEMPORARY ERRORS	18	0			59209	0	
F2XA3	CTRL	TEMPORARY ERRORS	27	0	58	0			
F2XA4	CTRL	TEMPORARY ERRORS			23	0	64214	0	

Figure 3-33A. NPDA Statistics Analysis (Trend)

3.1.3.7 CA MICS Class 7 Reports

These reports are not supported in the current release of the CA MICS Network Analyzer.

3.2 Sample Graphics

Sample Graphics are color graphic reports produced using SAS/GRAPH. The CA MICS Network Analyzer provides eleven Sample Graphics in three categories: service analysis, workload analysis, and reliability analysis.

Sample Graphics provide you with a sample set of reports from which you may develop other site-defined inquiries.

These inquiries are intended to illustrate a sampling of what you can do with network data.

You may make changes to report selection options, sequence patterns, and the content of these reports by modifying the code in `sharedprefix.MICS.SOURCE`, as required.

The list of possible Sample Graphics is provided in Figure 3-34. Descriptions of these reports and instructions on how to produce the Sample Graphics are discussed in the following sections:

- 1 - How to Produce Sample Graphics
- 2 - Sample Graphic Descriptions

Network Analyzer			
Sample Graphics Inquiry Reports			
Report Class	Report Name	Report Id	Data Base File
Service Analysis Reports	Average Response by Performance Class	SNTG101	SNTNSV
	Application Service Analysis by Hour	SNTG102	SNTPSY
	Application Service Analysis	SNTG103	SNTPSY
	Response Objective Results by Performance Class	SNTG104	SNTNSV
Workload Analysis Reports	Traffic Profile Report for Link	SNTG201	SNTNCL
	Communications Controller Utilization	SNTG202	SNTNAF
	NCP Buffer Utilization	SNTG203	SNTNAF
	Percent Link Utilization	SNTG204	SNTNCL
Reliability Analysis Reports	Error Count for Link	SNTG301	SNTNCL
	Percent Temporary Errors to Traffic	SNTG302	SNTNSF
	NPDA Events for Cluster Controller	SNTG303	SNTNEF

Figure 3-34. CA MICS Network Analyzer Graphic Inquiry List

3.2.1 How to Produce Sample Graphics

The CA MICS Network Analyzer Option Sample Graphics consist of eleven programs, each of which produces a single graph for a particular network component such as a link, a communications controller, or a cluster controller, or for an application. To generate one of the sample graphics, you must first tailor the program to your data center's conventions. This section describes how to tailor the graphic report programs and how to run them using the MICSSHR procedure.

Some selection options may be coded using macros provided in the report program. These are:

- o Report selection low time threshold
- o Report selection high time threshold
- o System Identifier (SYSID) selection
- o Network Identifier (NETWRKID) selection
- o Data base unit identifier selection

The database unit identifier selection is required, along with several other selection choices described later in this section.

REPORT PROGRAM STRUCTURE

Each sample graphics report is produced by a separate report program. The report programs, identified by name in Figure 3-34, are named SNTGcxx, where

c is the report class 1 = Service Analysis
 2 = Workload Analysis
 3 = Reliability Analysis

xx is a sequential report number

Each report program has the following sections:

* DEFINE DATA CENTER DEPENDENT DATA;

This section defines macros used in the data selection process. The macros provided are:

%LET SNTDLHR = 8;

Used to select low data time. Set to 8:00 AM in this case.

```
%LET SNTDHHR = 17;
```

Used to select high data time. Set to 5:00 PM in this case.

```
%MACRO SNTSYID;  
%MEND SNTSYID;
```

Used to select System ID. An example of code for this macro is:

```
%MACRO SNTSYID;  
  IF SYSID = 'T084';  
%MEND SNTSYID;
```

```
%MACRO SNTNEID;  
%MEND SNTNEID;
```

Used to select Network ID. An example of code for this macro is:

```
%MACRO SNTNEID;  
  IF NETWKID = 'TSONETWK';  
%MEND SNTNEID;
```

```
%LET SNTD = BSNTD;
```

Used to set the data base identifier. You must change the database identifier to correspond to the database unit from which the reports will be run. The database identifier is in the second position of the macro operand, B in this case. To change this for a CA MICS database unit with an identifier of C, merely change the B to a C, as below:

```
%LET SNTD = CSNTD;
```

To change the timespan selected for the graph, change the final character in the macro operand, D in this case, to one of the other acceptable timespans:

```
X - DETAIL  
D - DAYS (in this example)  
W - WEEKS
```

M - MONTHS
Y - YEARS

Remember that not all files in this product are supported in all timespans. See the file descriptions throughout Chapter 5 to determine if the file exists in your desired timespan.

For example, to select MONTHS data instead of DAYS data, change the D to M, as follows:

```
%LET SNTD = CSNTM;
```

*** SET OPTIONS;**

SAS and SAS/GRAPH options are set in this section. Remember that these graphs are set up to run with all supported versions of SAS, as documented in section 6.7 of the System Administrator Guide.

It is important to tell SAS/GRAPH software the device you are using for the graphs. This is done in the DEVICE= operand. IBM3279 is used in all sample routines.

A sample GOPTIONS statement is supplied below:

```
GOPTIONS CTITLE=GREEN DEVICE=IBM3279 BAUD=9600  
BORDER VPOS=40 COLORS=(WHITE);
```

*** COLLECT THE DATA;**

The SET statement determines which file and cycle will be selected. To change the cycle, modify the last two numeric values of the SAS data set name. The change from cycle 01 to cycle 03 is

```
BEFORE: SET &SNTD.SNTPSY01;
```

```
AFTER: SET &SNTD.SNTPSY03;
```

* SELECT DESIRED OBSERVATIONS;

SYSID, Network ID, time period, and network component or application are selected here.

You MUST select a network component or application here. The following table shows the Report-ID and the variable name that you select. Each report routine has an example coded in this section to guide you. Thus, in report SNTG103, Application Service Analysis by Hour, the sample selection statement is

IF PLU='CICSPROD' OR PLU='CICSTEST';

Select Variable	Report ID
NSVPCCLSS	SNTG101
PLU	SNTG102
PLU	SNTG103
NSVPCCLSS	SNTG104
NETNAME	SNTG201
NCPNAME	SNTG202
NCPNAME	SNTG203
NETNAME	SNTG204
NETNAME	SNTG301
NSFFRNAM	SNTG302
NEFFRNAM	SNTG303

Other selections may be coded in this section.

* PROCESSING;

Summarization and sequencing is performed in this section.

* SETUP VARIABLES FOR PRINTING;

The CALL SYMPUT function is used to set up macro variables for printing in the TITLE and FOOTNOTE statements.

* CHART THE DATA;

The SAS/GRAPH GCHART or GPLOT statements are defined in this section.

* DEFINE THE PATTERNS AND SYMBOLS;

Chart or Plot symbols and patterns are defined in this section.

* TITLE AND FOOTNOTES;

Titles and Footnotes are defined in this section.

PRODUCING THE SAMPLE GRAPHICS

The sample graphics described in the following sections are produced using the standard CA MICS CLIST, MICSSHRd where d is the database identifier of the database unit containing the CA MICS Network Analyzer Option. Follow the steps below to produce the graphic inquiries:

- ___ 1. Ensure that the version of SAS being invoked by the MICSSHRd procedure includes SAS/GRAPH software. (Note that SAS/GRAPH software is a separately licensed product.)
- ___ 2. To invoke Network Sample Graphics under SAS/GRAPH software, you must use a graphics terminal supported by SAS/GRAPH. Refer to the SAS/GRAPH documentation for a list of graphics devices supported by SAS/GRAPH software.
- ___ 3. Edit the graph program using ISPF or another similar editor and follow the steps outlined. This is best explained using a particular graph routine. We have chosen SNTG102. It may be useful to print a copy of this routine to review with this example.

Note that the mandatory steps are identified as REQUIRED in the left margin.

- Optional a. Select 7:00 AM as the low data timestamp and update the &SNTDLHR macro variable.

```
%LET SNTDLHR = 7;
```

- Optional b. Select 4:00 PM as the high data timestamp and update the &SNTDHHR macro variable.

```
%LET SNTDHHR = 16;
```

- Optional c. Select only data from system 'T033' and update the %SNTSYID macro.

```
%MACRO SNTSYID;  
    IF SYSID = 'T033';  
%MEND SNTSYID;
```

- Optional d. Select only data from network 'PRODNY01' and update the %SNTNEID macro.

```
%MACRO SNTNEID;  
    IF NETWRKID = 'PRODNY01';  
%MEND SNTNEID;
```

- REQUIRED e. Select the database unit identifier, D, and update the &SNTD macro variable.

```
%LET SNTD = DSNTD;
```

Note that there is no change made to the file timespan, so the DAYS timespan is selected.

- Optional f. Select the 02 cycle and update the SET statement in the * COLLECT THE DATA section of the program.

```
SET &SNTD.SNTPSY02;
```

- REQUIRED g. Select one or two applications to be displayed on the report (the data element name for application is primary logical unit (PLU)). Applications 'TSOPRIM' and 'TSOTEST' will be selected in the * SELECT DESIRED OBSERVATIONS section of the program.

```
IF PLU='TSOPRIM' OR PLU='TSOTEST';
```

IMPORTANT: Only programs SNTG102 and SNTG103 provide for selection of more than one network component or application. In all other graphic programs you may select only one component or application.

___ 4. Access SAS from the CA MICS Workstation Facility (MWF) main panel by selecting option 3, SAS With CA MICS Libraries. Then, from this panel select option 3, SAS with CA MICS Database Unit Selection. Next, you will be prompted by a panel where can select the the database unit at your site that contains the CA MICS Network Analyzer Option.

___ 5. Enter the following %INCLUDE statement when prompted by SAS:

```
%INCLUDE SOURCE(SNTG102);  
RUN;
```

3.2.2 Sample Graphics Descriptions

Each of the sample graphics is described in this section. Because this document is distributed in machine-readable form, we cannot show the actual graphic output.

These reports are discussed in the following sections:

- 1 - Average Response Time by Performance Class (SNTG101)
- 2 - Application Service Analysis by Hour (SNTG102)
- 3 - Application Service Analysis (SNTG103)
- 4 - Response Objective Results by Perf. Class (SNTG104)
- 5 - Traffic Profile Report for Link (SNTG201)
- 6 - Communications Controller Utilization (SNTG202)
- 7 - NCP Buffer Utilization (SNTG203)
- 8 - Percent Link Utilization (SNTG204)
- 9 - Error Count for Link (SNTG301)
- 10 - Percent Temporary Errors to Traffic (SNTG302)
- 11 - NPDA Events for Cluster Controller (SNTG303)

3.2.2.1 Avg. Response Time by Performance Class (SNTG101)

INTENDED USAGE:

This chart is used to determine the adequacy of service to the end-user on the basis of performance classifications established by the installation. A reference line is drawn on the graph to indicate the objective response time for the performance class.

FORMAT:

This display produces a line graph of average end-user response time by hour within ZONE for a given NLDM/RTM performance class.

DATA SOURCE (File/Timespan):

SNTNSV01/DAYS

DATA ELEMENTS USED:

ZONE, HOUR, NSVPCLSS, NSVAVTTM

CALCULATIONS:

None

USAGE CONSIDERATIONS:

Performance Class (NSVPCLSS) is an installation-defined classification used by NetView Logical Data Manager (NLDM) to accumulate response time. Section 6.3 provides guidelines on how to set up NLDM performance classes so that this report reflects service in the required categories.

3.2.2.2 Application Service Analysis by Hour (SNTG102)

INTENDED USAGE:

This chart is used to determine the relative amount of application response time which is consumed in the host compared to that consumed by the network for two applications.

FORMAT:

This display produces a block chart showing end-user response times for two primary logical units (PLUs) that are divided into their host and network components. The response for each PLU is shown for a two hour period.

DATA SOURCE (File/Timespan):

SNTPSY01/DAYS

DATA ELEMENTS USED:

HOURL, PLU, PSYAVHTM, PSYAVNTM

CALCULATIONS:

None

USAGE CONSIDERATIONS:

The source for this inquiry is NetView Performance Monitor (NPM) Session data, including host and network response time. NPM may not collect network response time (transit time in NPM terms) for all transactions so the actual average network time may be misleading. The NPM Service by Application Report (SNT101) displays PCT RESPONSES WITH NO NET RESP, the percentage of responses with no network response time. Refer to Section 3.1.3.1.1 for an explanation of this field. You may use the profile version of SNT101 to determine the completeness of the data displayed on the Graphic Inquiry.

Section 6.1.1.2 describes data from the NPM Session subsystem. Refer to the heading about network response time and definite response for further information.

3.2.2.3 Application Service Analysis (SNTG103)

INTENDED USAGE:

This chart is used to determine the relative amount of application response time which is consumed in the host compared to that consumed by the network for comparable applications.

FORMAT:

This display produces a horizontal bar chart indicating end-user response time for two primary logical units (PLUs), each divided into host and network response times for comparison.

DATA SOURCE (File/Timespan):

SNTPSY01/DAYS

DATA ELEMENTS USED:

HOURL, PLU, PSYAVHTM, PSYAVNTM

CALCULATIONS:

None

USAGE CONSIDERATIONS:

The source for this inquiry is NetView Performance Monitor (NPM) Session data, including host and network response time. NPM may not collect network response time (transit time in NPM terms) for all transactions so the actual average network time may be misleading. The NPM Service by Application Report (SNT101) displays PCT RESPONSES WITH NO NET RESP, the percentage of responses with no network response time. Refer to Section 3.1.3.1.1 for an explanation of this field. You may use The profile version of SNT101 to determine the completeness of the data displayed on the Graphic Inquiry.

Section 6.1.1.2 describes the data from the NPM Session subsystem. Refer to the heading about network response time and definite response for further information.

3.2.2.4 Response Objective Results by Perf. Class (SNTG104)

INTENDED USAGE:

Response objectives are established to provide measures of service. This graph illustrates how closely the installation came to meeting these objectives for a particular NLDM-defined performance class.

FORMAT:

This display produces a vertical bar chart showing the percentage of time response objectives were met within each hour. Response objectives are stated in seconds and hundredths of seconds, and the target response objective is identified in the graph footnote.

DATA SOURCE (File/Timespan):

SNTNSV01/DAYS

DATA ELEMENTS USED:

HOURL, NSVPCOBM, NSVPCCLSS, NLDRVAL, NSVPCOBJ,
NLDRVAL1-NLDRVAL4

CALCULATIONS:

None

USAGE CONSIDERATIONS:

Performance Class (NSVPCCLSS) is an installation-defined classification used by NetView Logical Data Manager (NLDM) to accumulate response time. Section 6.3 provides guidelines on how to setup NLDM performance classes so that this report reflects service in the required categories.

3.2.2.5 Traffic Profile Report for Link (SNTG201)

INTENDED USAGE:

This chart is used to determine the traffic load variation on a link over the course of a day. It also indicates the load due to retransmission of data.

FORMAT:

This display produces a stacked bar chart of input, output, and retransmitted traffic on the link by hour.

DATA SOURCE (File/Timespan):

SNTNCL01/DAYS

DATA ELEMENTS USED:

ZONE, HOUR, NCLNRCHR, NCLNRCHS, NCLNRRBY

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This inquiry is produced from NPM Network data. Note that the reference point for SENT, RECEIVED, and RETRANS (retransmitted data) is the host system, so SENT is usually the higher number. Retransmitted data is caused by errors between the sending and receiving nodes. You should investigate a noticeable bar for RETRANS since it may indicate a failing network component. You may review the inquiry Percent Temporary Errors to Traffic (SNTG302) to determine if the condition is caused by a failing link (line).

3.2.2.6 Communications Controller Utilization (SNTG202)

INTENDED USAGE:

This chart is used to determine the communications processor load variation over the course of a day.

FORMAT:

This display produces a line graph of communications controller processor percentage utilization by hour.

DATA SOURCE (File/Timespan):

SNTNAF01/DAYS

DATA ELEMENTS USED:

ZONE, HOUR, NAFPCCCU, NCPNAME

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This report is produced from NetView Performance Monitor (NPM) network data. The NPM Utilization by NCP Report (SNT208), provides additional information, such as "percent time in slowdown," which helps you to analyze the seriousness of highly-utilized communications controllers. See Section 3.1.3.2.3 for a description of SNT208.

3.2.2.7 NCP Buffer Utilization (SNTG203)

INTENDED USAGE:

This chart helps determine the adequacy and utilization of the memory in the communications control unit (CCU).

After the NCP load module (NCPGEN) is loaded into the CCU, the remaining memory is allocated for buffers. Thus, the buffering capability of the CCU is a function of the size of the NCPGEN and the amount of installed memory in the CCU. The maximum available NCP buffers value is the number of buffers initially allocated. The average free buffer queue length indicates the number of buffers that are generally available. The free buffer low-water mark is the lowest number of buffers that were available during the interval. The average free buffer count at slowdown is the the number of buffers that were left when the CCU became severely memory-constrained.

Network performance is being impaired if the free buffer low-water mark is consistently below the average free buffer count at slowdown. A memory upgrade (if possible) should be considered if the average free buffer queue length is consistently close to the average free buffer count at slowdown. Otherwise, some of the load on the CCU may have to be shifted to another unit.

FORMAT:

This display produces a line graph showing average free buffer queue length in the Network Control Program.

DATA SOURCE (File/Timespan):

SNTNAF01/DAYS

DATA ELEMENTS USED:

ZONE, HOUR, NAFVFBQ, NCPNAME

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This inquiry is produced from NetView Performance Monitor (NPM) Network data. Additional buffer statistics are provided on the NPM Utilization by NCP report (SNT208), described in Section 3.1.3.2.3.

3.2.2.8 Percent Link Utilization (SNTG204)

INTENDED USAGE:

This graph is used to determine the traffic fluctuation on a link over time. This helps you to determine the need for changes to the configuration, such as the addition of links or the upgrading of the link speed.

FORMAT:

This display produces a line graph displaying the percentage link utilization by hour for an individual boundary link.

DATA SOURCE (File/Timespan):

SNTNCL01/DAYS

DATA ELEMENTS USED:

HOURL, NETNAME, NCLPCLBS

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This report is produced from NetView Performance Monitor (NPM) Network data. Percent Link Utilization is based on the specification of link speed in an NCP generation parameter. If the actual speed of the link is different than that specified for the NCP because the value has not been updated to reflect a hardware upgrade or because modems in use on the link are adjusting the link speed dynamically, the percentage displayed on this inquiry will be in error.

3.2.2.9 Error Count for Link (SNTG301)

INTENDED USAGE:

This chart is used to visualize the changes in the line quality over the course of a time-zone.

FORMAT:

This display produces a line graph showing error counts per hour for an individual link.

DATA SOURCE (File/Timespan):

SNTNCL01/DAYS

DATA ELEMENTS USED:

ZONE, HOUR, NCLNRERR, NETNAME

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This inquiry is produced from NetView Performance Monitor (NPM) Network data. It reflects the count of temporary errors detected for network line components by the network control program during this measurement interval. You may correlate this inquiry with the NPM/NCP Utilization by Link report (SNT209) described in Section 3.1.3.2.4. SNT209 provides additional transmission, polling, error, and utilization information.

3.2.2.10 Percent Temporary Errors to Traffic (SNTG302)

INTENDED USAGE:

Increases in the percentage of temporary errors to total line traffic over time may mean that a particular link is degrading and should be examined.

FORMAT:

This display produces a line graph showing the percentage of temporary errors to total line traffic as reported by NPDA.

DATA SOURCE (File/Timespan):

SNTNSF01/DAYS

DATA ELEMENTS USED:

HOURL, NSFFRNAM, NSFPCERR

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This inquiry is produced from NetView Problem Determination Application (NPDA) data. An increase in the ratio of temporary errors to character traffic on the line may indicate a failing network component somewhere along the line, and should be investigated. You may correlate this inquiry with the NPM NCP Utilization by Link report (SNT209) described in Section 3.1.3.2.4. SNT209 provides additional transmission, polling, error, and utilization information from NPM network data.

3.2.2.11 NPDA Events for Cluster Controller (SNTG303)

INTENDED USAGE:

Events are recorded because the percent of temporary errors to line traffic threshold has been exceeded or because some other user-defined incident has occurred. A high or increasing number of events over time may lead to a detailed investigation of the NPDA data for the cluster controller identified in this inquiry.

FORMAT:

This display produces a line graph of the number of installation-defined Events recorded by NPDA in each hour of the selected time period.

DATA SOURCE (File/Timespan):

SNTNEF01/DAYS

DATA ELEMENTS USED:

HOURL, NEFFRNAM, NEFNREVT

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This inquiry is produced from NetView Problem Determination Application (NPDA) data. You may investigate the NPDA Event Analysis report (SNT601), described in Section 3.1.3.6.1, to obtain the cause of each DETAIL event.

3.3 MICF Inquiries

The CA MICS Network Analyzer provides a set of precomposed report and color graphics inquiries categorized for analysis by service, reliability, performance, and workload. These inquiries provide an immediate source of useful reporting and color graphics presentations, and are implemented using the CA MICS Information Center Facility (MICF). You may tailor the output from these inquiries using Execution Time Data Selection panels. In addition, you may develop customized reports for your installation with a minimum of effort by modifying copies of the distributed inquiries.

The distributed inquiry names have been designed for ease of identification. Each name identifies the component being reported on, the type of output it has (i.e., color graphics, printer graphics, or printed reports), and the timespan it is produced from (i.e., daily, weekly, monthly). It also has its own unique identifier to distinguish it from other unique inquiries of the same type.

Consider, for example, the MICF inquiry SNTCDI:

- 1) SNT indicates that the inquiry comes from the CA MICS Network Analyzer.
- 2) C indicates that the output is color graphics.
- 3) D indicates that the timespan is DAYS.
- 4) I is an alphabetic identifier that distinguishes the inquiry from other CA MICS Network MICF inquiries that also have color graphics output and are produced from the DAYS timespan.

The list of distributed MICF inquiries, instructions on how to modify them, and descriptions of the output that they produce are provided in the following sections:

- 1 - MICF Inquiry Descriptions
- 2 - How to Modify Standard MICF Inquiries

3.3.1 MICF Inquiry Descriptions

All distributed MICF inquiries are categorized by analysis group. The CA MICS Network Analyzer provides MICF inquiries within five analysis groups: service, reliability, performance, workload, and resource. Figures 3-35, 3-35A, and 3-35B list the MICF inquiries contained within each of these groups.

- 1 - Service Analysis Inquiries
- 2 - Reliability Analysis Inquiries
- 3 - Performance Analysis Inquiries
- 4 - Workload Analysis Inquiries
- 5 - Resource Analysis Inquiries

CA MICS Network Analyzer						
MICF Distributed Inquiries						
Report Class	Report Name	Report ID		Database File		
		Color Graphics	Printer Graphics			
Service	*NetView Daily Avg Resp by PCLASS	SNTCD1	SNTPD1	SNTNSV		
	*NetView Daily % Resp Within Obj by PCLASS	SNTCD4	SNTPD4	SNTNSV		
	*NetView Daily Avg Response by Link	SNTCDI	SNTPDI	NVSNULL		
	*NetView Daily % Resp Within Obj by Link	SNTCDN	SNTPDN	NVSNULL		
	NetSpy Daily PLU Resp Time Components	SNTCD5	SNTPD5	SNTNSP		
	NetSpy Daily SLU Resp Time Components	SNTCDT	SNTPDT	SNTNSS		
	*NetView Application Service/Workload Ranking	(SNTLDA, SNTLDB)		SNTNSA, SNTRTM		
	*NetView Application Service/Workload Ranking	(SNTLD6, SNTLD7)		SNTLSY		
	*NetView Link Service/Workload Ranking	(SNTLD8, SNTLD9)		SNTNLL		
	*NetView PCLASS Service/Workload Ranking	(SNTLDC, SNTLDD)		SNTNSV		
	NPM Application Service/Workload Ranking	(SNTLD0, SNTLD1)		SNTPSU		
	NPM Link Service/Workload Ranking	(SNTLD0, SNTLD1)		SNTNPL		
	NPM Application/Link Service/Workload Ranking	(SNTLD0, SNTLDR)		SNTNPL		
	NetSpy Application Service/Workload Ranking	(SNTLD2, SNTLD3)		SNTNSP		
	TS0 Resp Time Components	SNTCD0	SNTPD0	SNTNSP, TS0TSU		
	Reliability	NPM Daily Link Error Count	SNTCD9		SNTNCL	
		NPM/NetSpy Daily Link Error Count		SNTPD9	SNTNCL	
*NetView Daily % Link Errors to Traffic		SNTCDA	SNTPDA	SNTNSF		
*NetView Daily NPDA Events Summary		SNTCDB	SNTPDB	SNTNEF		
NPDA Daily Alerts By Problem Type		SNTCDL	SNTPDL	SNTNEF, SNTNSF,		
				SNTGAF, SNTLNF		
NPDA Daily Alerts By Resource Type		SNTCDM	SNTPDM	SNTNEF, SNTNSF,		
				SNTGAF, SNTLNF		
*NetView Weekly Abnormal UNBINDs by PLU		SNTCWJ		NVSVBF		
*NetView Weekly Abnormal UNBIND Report			SNTLW0	NVSVBF		
*NetView Events Ranking		(SNTLDG, SNTLDH)		SNTNEF		
*NetView Events by Resource Type Ranking		(SNTLDI, SNTLDJ)		SNTNEF		
*NetView Events by Resource Ranking		(SNTLDO, SNTLDP)		SNTNEF		
NPDA Daily Resource Alert Summary			SNTLDT	SNTNEF, SNTNSF,		
				SNTGAF, SNTLNF		
NPDA Daily Resource Alert Description			SNTLDU	SNTNEF, SNTNSF,		
				SNTGAF, SNTLNF		
NPDA Daily Generic Alert Report		SNTLDV	SNTNEF, SNTNSF,			
			SNTGAF, SNTLNF			
*All reports beginning with NetView may also be produced from data collected by CA NetMaster.						

Figure 3-35. Network Analyzer MICF Inquiry List (Part 1 of 3)

CA MICS Network Analyzer					
MICF Distributed Inquiries					
Report Class	Report Name	Report ID		Database File	
		Color Graphics	Printer Graphics		
Performance	NPM Daily Pct. NCP Cycle Utilization	SNTCD6	SNTPD6		SNTNAF
	NPM Daily NCP Buffer Utilization	SNTCD7	SNTPD7		SNTNAF
	NPM Daily Link Utilization	SNTCD8			SNTNCL
	NetSpy Daily Pct. Time VR Held/Blocked	SNTCDZ	SNTPDZ		SNTNVR
	NetSpy Daily Average VR Response Time	SNTCD5	SNTPD5		SNTNVR
	NetSpy Daily Pct. NCP Cycle Utilization	SNTCDP	SNTPDP		SNTNAF
	NetSpy Daily NCP Buffer Utilization	SNTCDQ	SNTPDQ		SNTNAF
	NetSpy Daily Link Utilization	SNTCDR			SNTNCL
	Under/Over Utilized Line Analysis		SNTLDS		SNTNCL
	NetSpy/NPM Link Ranking By (Zone/Hour)	(SNTLDX, SNTLDY)			SNTNCL
	NCP Utilization Ranking	(SNTLDE, SNTLDF, SNTLXE, SNTLXF)			SNTNAF
	NetSpy/NPM Daily Link Utilization		SNTPDR		SNTNCL
Workload	*NetView Daily Connect Time by SNTACT1	SNTCDC			NVSNSC
	*NetView Daily Chars/1000 by SNTACT1	SNTCDD			NVSNSC
	*NetView Daily Data Chars/1000 by VR	SNTCDE			NVSRTE
	*NetView Daily Data Chars/1000 by SNTACT1	SNTCDF			NVSNSA
	*NetView Daily Cntl Chars/1000 by SNTACT1	SNTCDG			NVSNSA
	*NetView Weekly Cntl PIU Traffic by PLU	SNTCWH			NVSLSY
	*NetView Weekly Data PIU Traffic by PLU	SNTCWK			NVSLSY
	*NetView Daily Link Rank Report	SNTLDL			NVSNLL
	*NetView Daily PLU Rank Report	SNTLDM			NVSLSY
	NSA/NGA Daily Chars/1000 by SNTACT1	SNTCDX	SNTPDX		SNTNAC
	NSA/NGA Daily PIU Traffic by SNTACT1	SNTCDY	SNTPDY		SNTNAC
*All reports beginning with NetView may also be produced from data collected by CA NetMaster.					

Figure 3-35A. Network Analyzer MICF Inquiry List (Part 2 of 3)

CA MICS Network Analyzer					
MICF Distributed Inquiries					
Report Class	Report Name	Report ID		Database File	
		Color Graphics	Printer Graphics		
Resource	TCP/IP Daily In Byte Count By Hour		SNTPD2	TCPSTN	
	TCP/IP Daily Out Byte Count By Hour		SNTPD3	TCPSTN	
	TCP/IP Monthly In Byte Count By Zone		SNTPM1	TCPSTN	
	TCP/IP Monthly Out Byte Count By Zone		SNTPM2	TCPSTN	
	TCP/IP Daily Bytes Trans./Hour (CSV)	SNTEM1		TCPSTN	
	TCP/IP Daily Bytes Trans./Hour (CSV)	SNTEM2		TCPSTN	
	Chart CCU/Buffers/Slowdown by Hour		SNTPDU	SNTNAF	
	Plot CCU/Buffers/Slowdown by Hour		SNTPDV	SNTNAF	
	Plot NCP Hold/Intermediate Queue Length Plot		SNTPDW	SNTNAF	
*All reports beginning with NetView may also be produced from data collected by CA NetMaster.					

Figure 3-35B. Network Analyzer MICF Inquiry List (Part 3 of 3)

3.3.1.1 Service Analysis Inquiries

Service analysis inquiries indicate the level of service provided by a network to any given group of users. The service analysis inquiries are explained in greater detail in the following sections:

- 1 - NetView Daily Avg Resp by PCLASS
- 2 - NetView Daily % Resp Within Obj by PCLASS
- 3 - NetView Daily Avg Resp by Link
- 4 - NetView Daily % Resp Within Obj by Link
- 5 - NetSpy Daily PLU Resp Time Components
- 6 - NetSpy Daily SLU Resp Time Components
- 7 - NetView Application Service/Workload Ranking
- 8 - NetView Link Service/Workload Ranking
- 9 - NetView PCLASS Service/Workload Ranking
- 10 - NPM Application Service/Workload Ranking
- 11 - NPM Link Service/Workload Ranking
- 12 - NPM Application/Link Service/Workload Ranking
- 13 - NetSpy Application Service/Workload Ranking
- 14 - TSO Response Time Components

3.3.1.1.1 NetView Daily Avg Resp by PCLASS

INTENDED USE:

This chart indicates the adequacy of service to the end-user based on performance classifications (PCLASS) that are established by the data center. A reference line is drawn on the chart to indicate the objective response time for the performance class.

This inquiry is similar to the NetView Daily Avg Resp by PCLASS (SNTPD1) except that this inquiry produces graphical output using SAS/Graph, while SNTPD1 produces printer graphics using PROC CHART.

FORMAT:

This display produces a vertical bar chart showing average end-user response time (as measured by the 3274/3174 Response Time Monitor) by hour for a given Tivoli NetView Session Monitor (NLDM) performance class.

INQUIRY ID:

Color Graphics: SNTCD1
Printer Graphics: SNTPD1

DATA SOURCE (File/Timespan):

SNTNSV01 - Previous day

DATA ELEMENTS USED:

HOURL, NSVAVTTM, NSVPCLSS

CALCULATIONS:

None

USAGE CONSIDERATIONS:

Performance Class (NSVPCLESS) is a site-defined classification used by Tivoli NetView Session Monitor (NLDM) to accumulate response time. Sections 6.3.1 and 6.4.3 provide guidelines on how to set up performance classes.

The report volume may be large if generated without any selection criteria, depending on the number of links in your network environment.

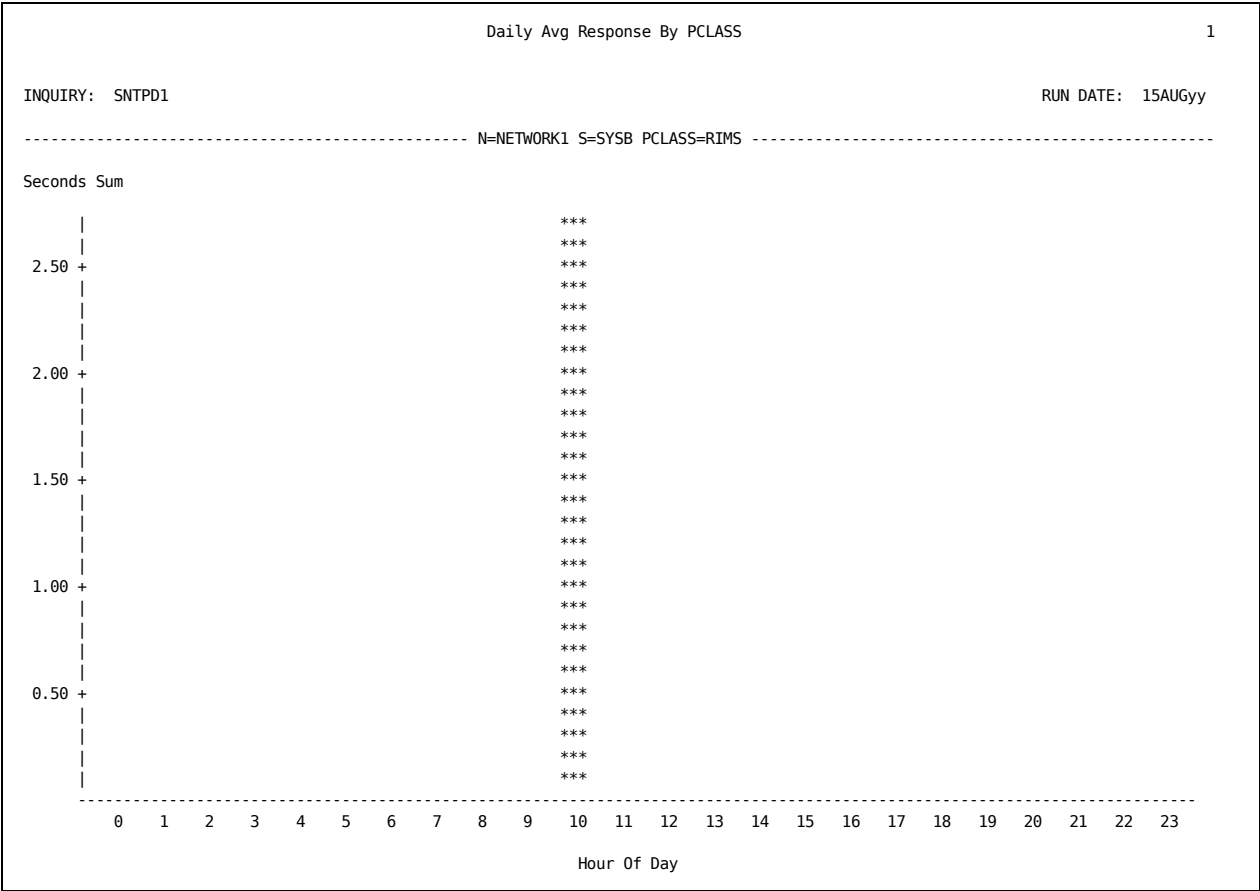


Figure 3-

3.3.1.1.2 NetView Daily % Resp Within Obj by PCLASS

INTENDED USE:

Response objectives are established to provide measures of service. This chart illustrates how close the data center comes to meeting the objectives for a Tivoli NetView Session Monitor (NLDM) defined performance class.

FORMAT:

This display produces a vertical bar chart showing the percentage of time the response objectives are met within an hour (as measured by the 3274/3174 Response Time Monitor) for a given NetView Session Monitor (NLDM) performance class.

INQUIRY ID:

Color Graphics: SNTCD4
Printer Graphics: SNTPD4

DATA SOURCE (File/Timespan):

SNTNSV01 - Previous day

DATA ELEMENTS USED:

HOURL, NSVPCOBM, NSVPCLSS

CALCULATIONS:

None

USAGE CONSIDERATIONS:

Performance Class (NSVPCLSS) is a site-defined classification used by NetView Session Monitor (NLDM) to accumulate response time. Sections 6.3.1 and 6.4.3 provide guidelines on how to set up performance classes.

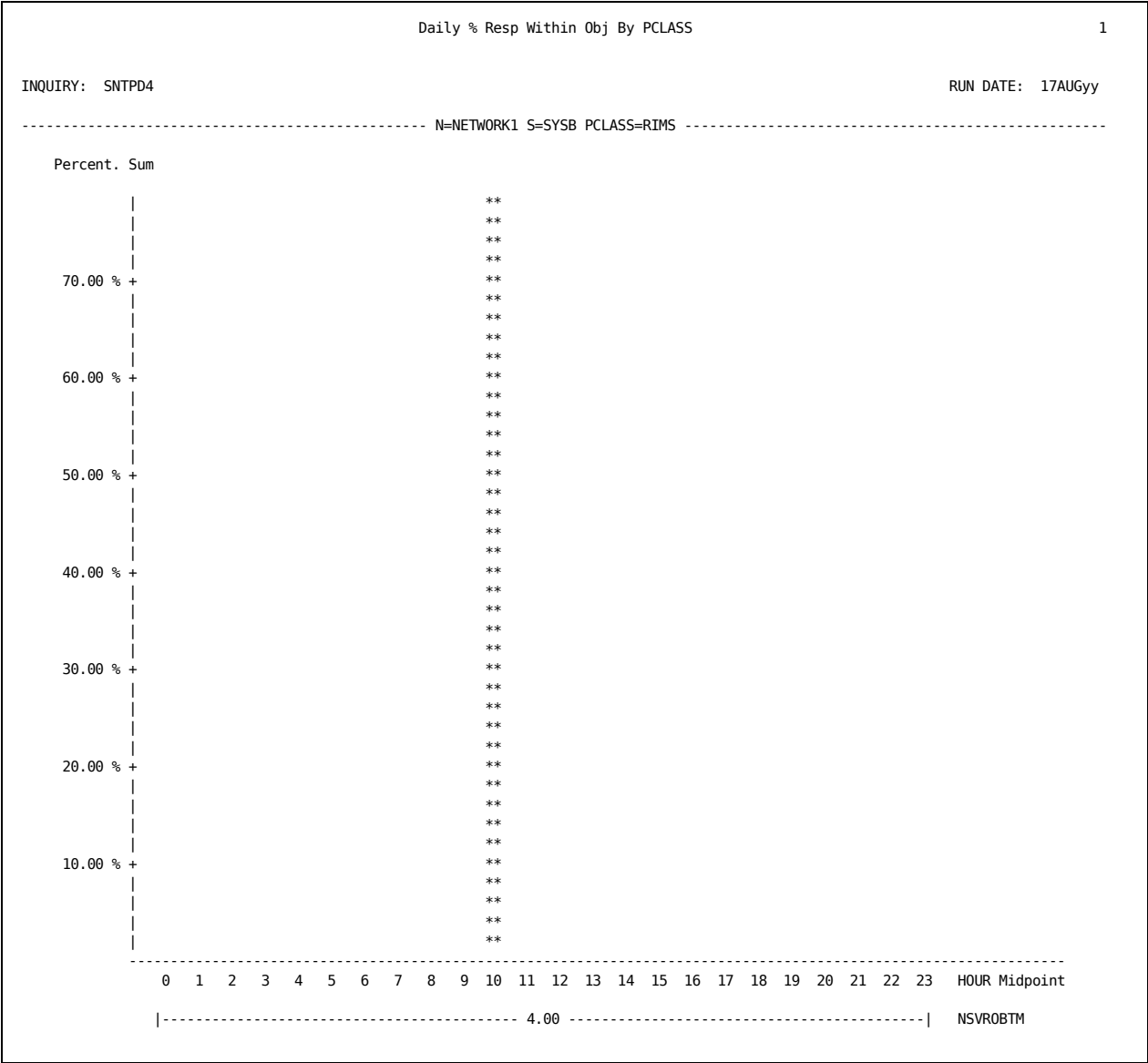


Figure 3-

3.3.1.1.3 NetView Daily Avg Resp by Link

INTENDED USE:

This chart shows average end-user response time for all terminals that are attached on a link to a 3274/3174 equipped with a Response Time Monitor. This MICF inquiry summarizes average response time independent of the performance classes that are defined within Tivoli NetView Session Monitor (NLDM) for the terminal-to-host sessions across this link. You can use this chart to determine which links offer the shortest or longest average response times within the network. You can also use the chart in conjunction with MICF inquiry SNTCD8 to compare average response time with utilization for a given link.

FORMAT:

This display produces a vertical bar chart of average end-user response time (as measured by the 3274/3174 Response Time Monitor) by hour for a given SLULINK, the peripheral link to which a remote terminal is attached.

INQUIRY ID:

Color Graphics: SNTCDI
Printer Graphics: SNTPDI

DATA SOURCE (File/Timespan):

NVSNLL01 - Previous day

DATA ELEMENTS USED:

HOURL, NLLAVTTM, SLULINK

CALCULATIONS:

None

USAGE CONSIDERATIONS:

Since this chart is based on the measurement of end-to-end average response time and not on the network component's average response time, it may indicate that there is poor response by link for delays caused by events outside the network.

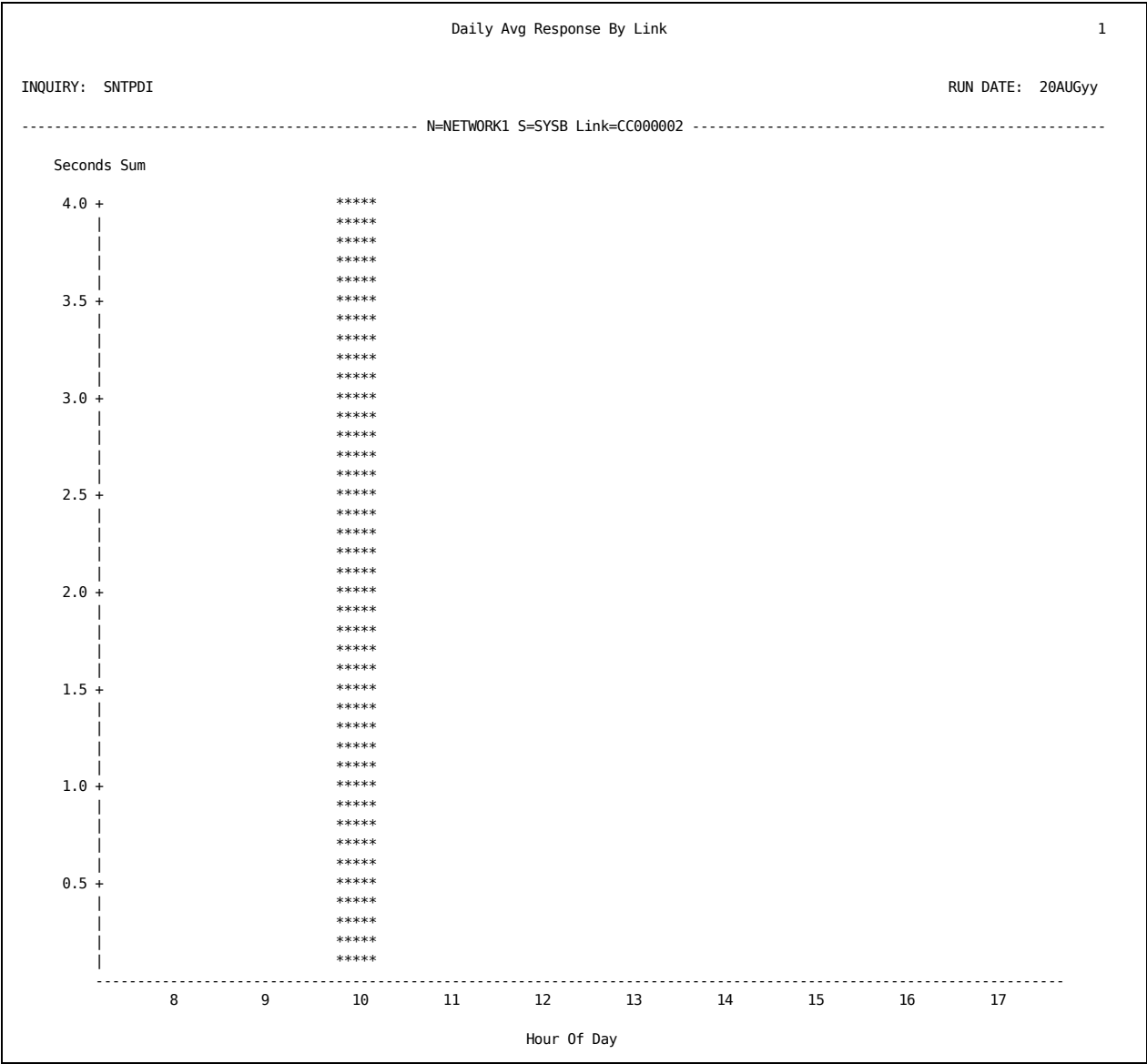


Figure 3-

3.3.1.1.4 NetView Daily % Resp Within Obj by Link

INTENDED USE:

Response objectives are established to provide measures of service. This chart illustrates how close the data center comes to meeting the objectives for all the NetView Session Monitor/NLDM-defined performance classes that are defined for the terminal to host sessions across a given link. For this chart, Percent Responses within Objective (NLLPCOBM) is summarized across the performance classes defined for the terminal-to-host sessions on the link.

FORMAT:

This display produces a vertical bar chart showing the percentage of time the response objectives are met within each hour (as measured by the 3274/3174 Response Time Monitor) for a given SLULINK, the peripheral link to which a remote terminal is attached.

INQUIRY ID:

Color Graphics: SNTCDN
Printer Graphics: SNTPDN

DATA SOURCE (File/Timespan):

NVSNLL01 - Previous day

DATA ELEMENTS USED:

HOURL, NLLPCOBM, SLULINK

CALCULATIONS:

None

USAGE CONSIDERATIONS:

Since this chart is based on the measurement of end-to-end response time and not on the network component's response time, it may indicate that there is poor response by link for delays caused by events outside the network.

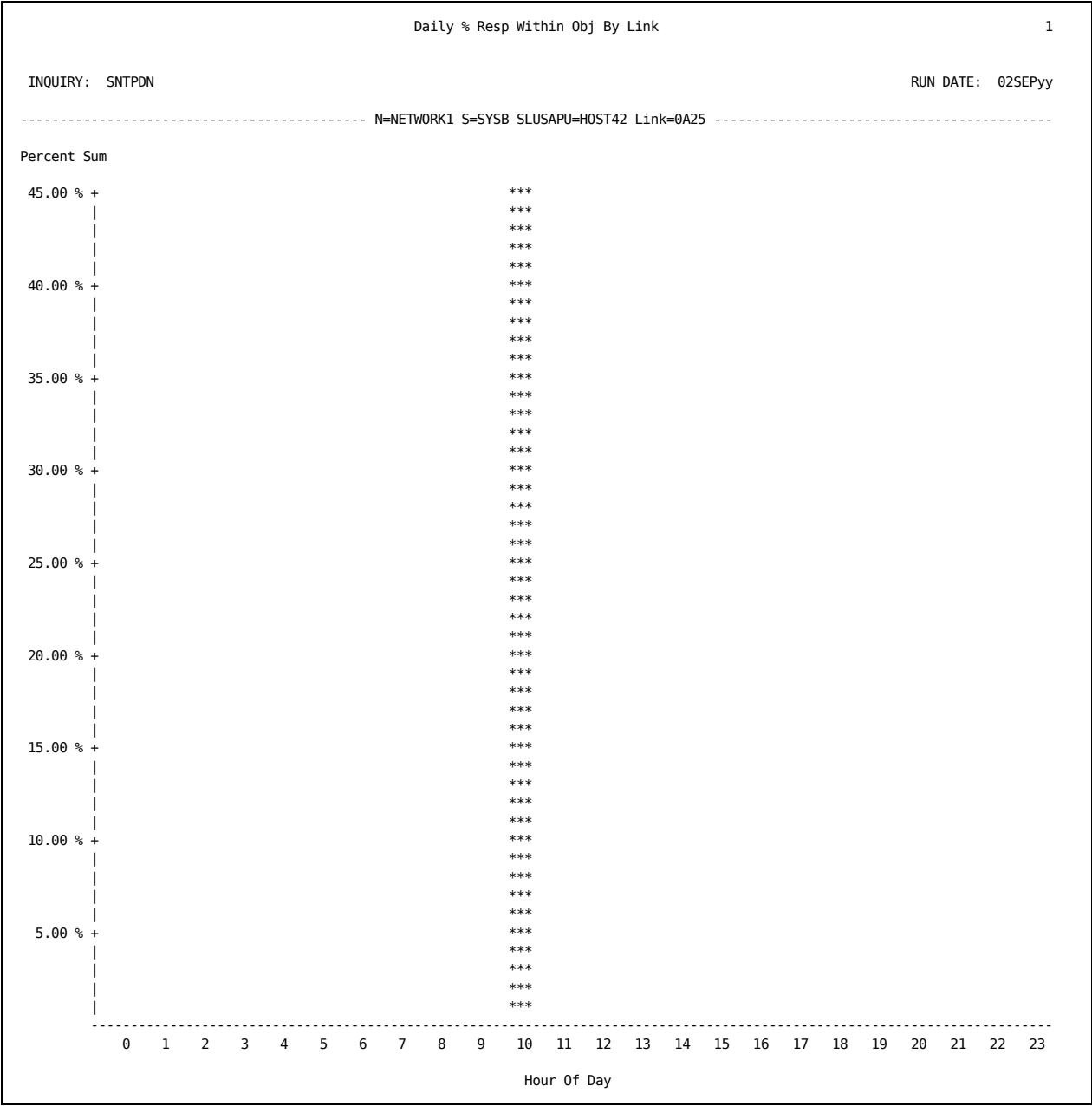


Figure 3-

3.3.1.1.5 NetSpy Daily PLU Resp Time Components

INTENDED USE:

This chart is used to determine, for a given application, what portion of average total response time occurs in the host versus that which occurs in the network.

FORMAT:

This display produces a stacked vertical bar chart showing the components of average total response time (host and network) by hour for a given application.

INQUIRY ID:

Color Graphics: SNTCDS
Printer Graphics: SNTPDS

DATA SOURCE (File/Timespan):

SNTNSP01 - Previous day

DATA ELEMENTS USED:

HOURL, PLU, NSPAVHTM, NSPAVNTM

CALCULATIONS:

None

USAGE CONSIDERATIONS:

The source for this inquiry is the CA NetSpy VTAM interface data.

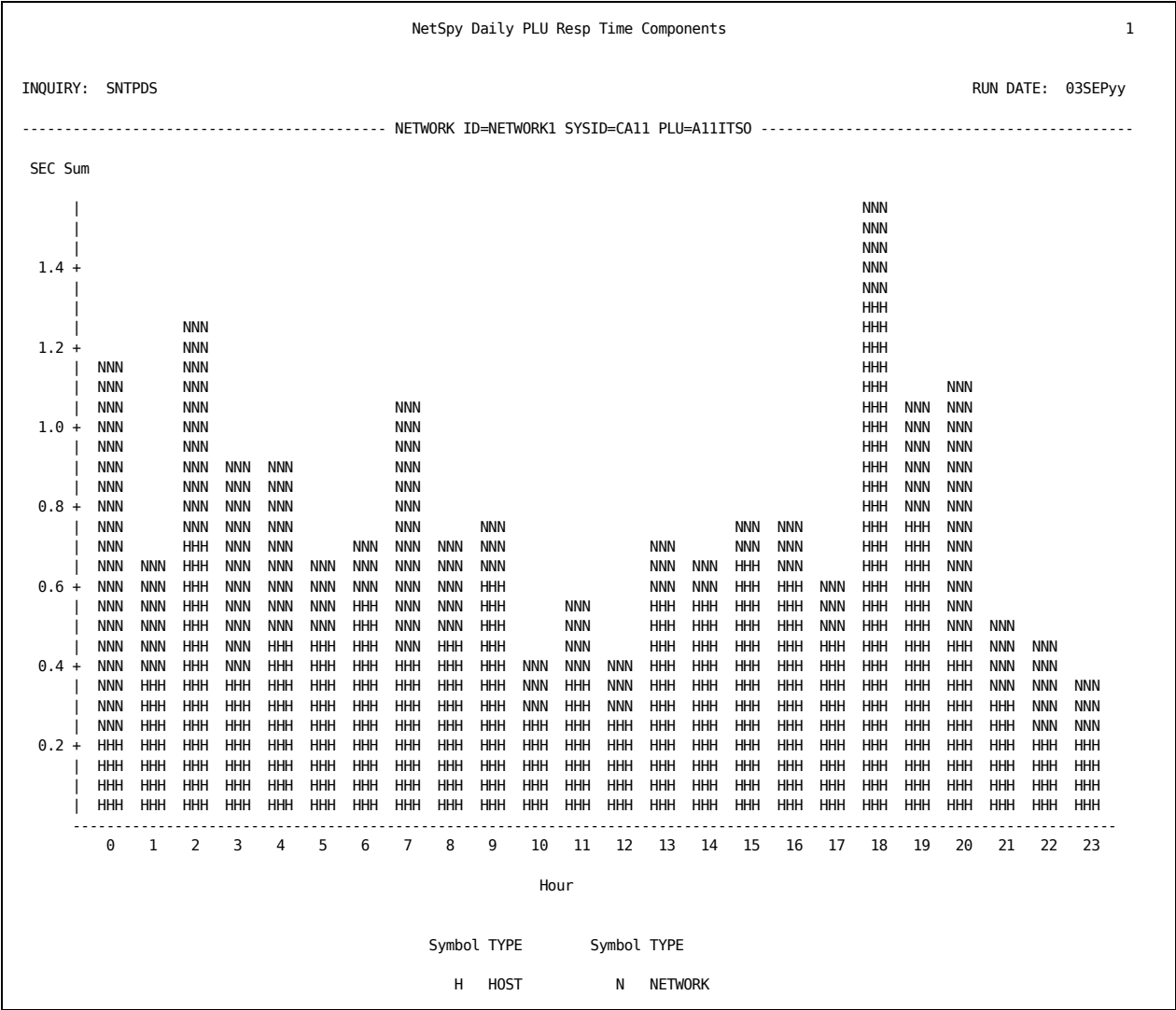


Figure 3-

3.3.1.1.6 NetSpy Daily SLU Resp Time Components

INTENDED USE:

Use this chart to determine, for a given terminal, what portion of average total response time occurs in the host versus that which occurs in the network.

FORMAT:

This display produces a stacked vertical bar chart showing the components of average total response time (host and network) by hour for a given terminal.

INQUIRY ID:

Color Graphics: SNTCDT

Printer Graphics: SNTPDT

DATA SOURCE (File/Timespan):

SNTNSS01 - Previous day

DATA ELEMENTS USED:

hour, SLU, NSSAVHTM, NSSAVNTM

CALCULATIONS:

None

USAGE CONSIDERATIONS:

The source for this inquiry is the CA NetSpy VTAM interface data.

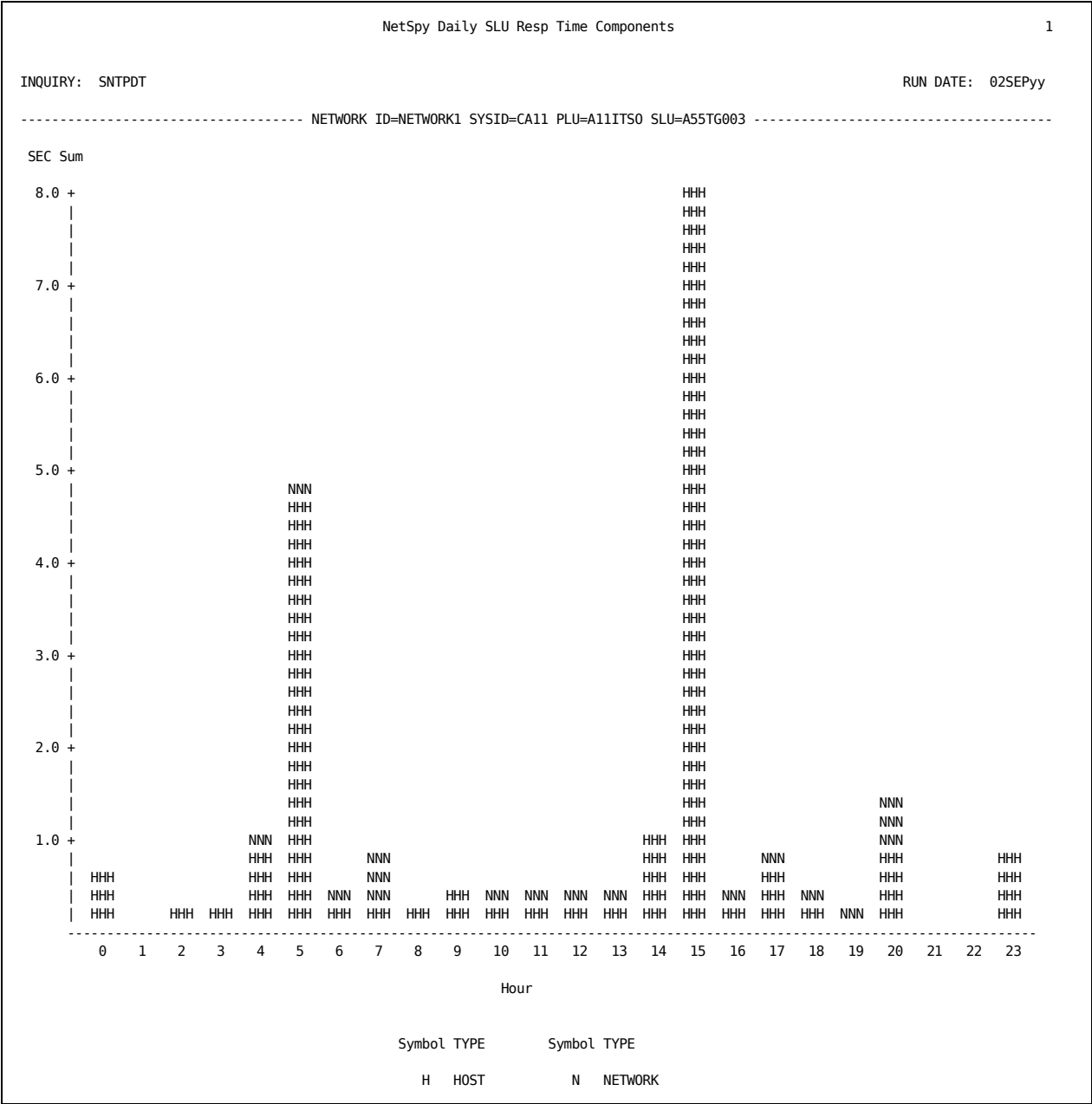


Figure 3-

3.3.1.1.7 NetView Application Service/Workload Ranking

INTENDED USE:

To rank application workloads in ascending or descending order based on response times or character volumes. The user chooses the number of applications ranked, the order of ranking, and the variable used to rank on. The report provides both response and workload information that can be used in determining possible bottlenecks and/or poor response times.

FORMAT:

A 17 column report approximately 132 characters wide. Best suited for hardcopy review but can be reviewed online. The information is summarized and presented by NETWRKID, SYSID, SNTACT1, Data Range, and Zone or Zone by Hour.

INQUIRY ID:

SNTLDA - Application w/in zone - NVSNSA/NVSRTM files
SNTLDB - Application w/in hour - NVSNSA/NVSRTM files
SNTLD6 - Application w/in zone - SNTNPL file
SNTLD7 - Application w/in hour - SNTNPL file

DATA SOURCE (File/Timespan):

NVSNSA/NVSRTM Days
SNTNPL Days

DATA ELEMENTS USED:

SNTLDA/SNTLDB

DURATION, SNTACT1, RTMAVTTM, OBJECTIV, RTMNRNR, RTMTRSMN, RTMPCOBS, RTMPCOBT, RTMTRESC, SAMPLES, NSATOTSN, NSATOTRC, NSATOTTR, NSAAVCHS, NSAAVCHR, NSAAVCHT, NSAAVPIU, SYSID, NETWRKID, DATA, ZONE, RANKELEM, RANKLBL, CURRENT, DATE, IQ, TIME, HOUR

SNTLD6/SNTLD7

DURATION, PLU, LSYAVTTM, OBJECTIV, LSYNRNR, LSYTRSMN, LSYPCOBS, LSYPCOBT, LSYTRESC, SAMPLES, LSYTOSN, LSYTOTRC, LSYTOTTR, LSYAVCHS, LSYAVCHR, LSYAVVHT, LSYAVPIU, NETWRKID, SYSID, DATA, ZONE, RANKELEM, RANKLBL, DATE TIME, IQ,

CURRENT, HOUR

CALCULATIONS:

SNTLDA/SNTLDB

```

/* Data Element Derivation (DATE) */;
FORMAT DATE DATE7.;
LABEL DATE="Date Selection Field";
DATE = DATEPART(ENDTS);
;
/* Data Element Derivation (TIME) */;
FORMAT TIME TIME11.2;
LABEL TIME="Time Selection Field";
TIME = TIMEPART(ENDTS);
;
/* Data Element Derivation (DATA) */;
LENGTH DATA $15;
FORMAT DATA $CHAR15.;
LABEL DATA="DATA RANGE";
DATA = ' ';
/* SAS System Statements (Load DATA Variable) */;
RETAIN DATEA DATEB;
LENGTH DATEA DATEB 4.;
IF SESTYPE =:'LU-LU' THEN DO;
    DATEA = MIN(DATEA,STARTTS);
    DATEB = MAX(DATEB,ENDTS);
END;
IF _EOF_ THEN DO;
    DATEA=DATEPART(DATEA);
    DATEB=DATEPART(DATEB);
    SUBSTR(DATA,1,7)=PUT(DATEA,DATE7.);
    SUBSTR(DATA,8,1)='- ';
    SUBSTR(DATA,9,7)=PUT(DATEB,DATE7.);
    DROP DATEA DATEB;
    CALL SYMPUT('S',DATA);
    %GLOBAL S;
END;
IF SESTYPE =:'LU-LU';
/* Data Summarization */
%MACRO NEGATE;
    DATA=SYMGET('S');
%MEND NEGATE;
;
/* Data Element Derivation (IQ, &I) */;
LENGTH IQ $8;
FORMAT IQ $CHAR8.;
LABEL IQ="INQUIRE NAME";

```

```
IQ = ' ';
SUBSTR(IQ,1,1)='(';
SUBSTR(IQ,2,6)=SYMGET('INQINAME');
SUBSTR(IQ,8,1)=')';
CALL SYMPUT('I',PUT(IQ,$CHAR8.));
%GLOBAL I;
;
/* Data Element Derivation (CURRENT, &C) */;
FORMAT CURRENT WEEKDATE15.;
LABEL CURRENT="CURRENT DATE";
CURRENT = TODAY();
C=PUT(CURRENT,WEEKDATE15.);
C=COMPRESS(C) ;
CALL SYMPUT('C',PUT(C,$CHAR12.));
%GLOBAL C;
;
/* Data Element Derivation (OBJECTIV) */;
LENGTH OBJECTIV $12;
FORMAT OBJECTIV $CHAR12.;
LABEL OBJECTIV="X PERCENT OF RESPONSE WITHIN XX SECONDS";
OBJECTIV = ' . '; IF RTMPCOBJ GE 0 OR RTMROBTM GE
0 THEN DO; SUBSTR(OBJECTIV,1,3)=PUT(RTMPCOBJ,3.);
SUBSTR(OBJECTIV,4,4)='% < ';
SUBSTR(OBJECTIV,8,5)=PUT(RTMROBTM,4.1); END; ; /* Data
Element Derivation (RANKELEM) */; FORMAT RANKELEM 8.;
LABEL RANKELEM="&RL"; RANKELEM = &RANKELEM; ; /* Data
Element Derivation (RANKLBL) */; LENGTH RANKLBL $40;
FORMAT RANKLBL $CHAR40.; LABEL RANKLBL="LABEL OF RANKING
ELEMENT"; RANKLBL = SYMGET('RL'); ; /* Data Element
Derivation (RTMPCOBS) */; LENGTH RTMPCOBS $4; FORMAT
RTMPCOBS $CHAR4.; LABEL RTMPCOBS="% MET OF SAMPLED";
RTMPCOBS = ' . '; IF RTMPCOBM GE 0 THEN DO;
SUBSTR(RTMPCOBS,1,3)=PUT(RTMPCOBM,3.);
SUBSTR(RTMPCOBS,4,1)='%'; END; ; /* Data Element
Derivation (RTMPCOBT) */; LENGTH RTMPCOBT $4; FORMAT
RTMPCOBT $CHAR4.; LABEL RTMPCOBT="% MET OF TOTAL";
RTMPCOBT = ' . '; IF RTMPCTR4 GE 0 THEN DO;
SUBSTR(RTMPCOBT,1,3)=PUT(RTMPCTR4,3.);
SUBSTR(RTMPCOBT,4,1)='%'; END; ; /* Data Element
Derivation (RTMTRSMN) */; FORMAT RTMTRSMN SCALE4.; LABEL
RTMTRSMN="TRANSACTIONS PER MINUTE"; RTMTRSMN = .;
DURMINS=(DURATION/60); IF DURMINS GT 0 THEN
RTMTRSMN=RTMTRESC/DURMINS; ; /* Data Element Derivation
(NSATOTSN) */; FORMAT NSATOTSN SCALE4.; LABEL
NSATOTSN="TOTAL CHARACTERS SENT"; NSATOTSN =
SUM(NSANRCBS,NSANRTBS); ; /* Data Element Derivation
(NSATOTRC) */; FORMAT NSATOTRC SCALE4.; LABEL
NSATOTRC="TOTAL CHARACTERS RECEIVED"; NSATOTRC =
SUM(NSANRCBR,NSANRTBR); ; /* Data Element Derivation
```

```

(NSATOTTR) */; FORMAT NSATOTTR SCALE4.; LABEL
NSATOTTR="TOTAL CHARACTERS TRANSMITTED"; NSATOTTR =
SUM(NSANRCBR,NSANRTBR,NSANRCBS,NSANRTBS); ; /* Data
Element Derivation (NSAAVCHS) */; FORMAT NSAAVCHS SCALE4.;
LABEL NSAAVCHS="AVERAGE CHARACTERS SENT"; NSAAVCHS = .;
NSANRFSR=SUM(NSANRCBS,NSANRTBS); IF RTMTRESC GT 0 THEN
NSAAVCHS=NSANRFSR/RTMTRESC; ; /* Data Element Derivation
(NSAAVCHR) */; FORMAT NSAAVCHR SCALE4.; LABEL
NSAAVCHR="AVERAGE CHARACTERS RECEIVED"; NSAAVCHR = .;
NSANRFRE=SUM(NSANRCBR,NSANRTBR); IF RTMTRESC NE 0 THEN
NSAAVCHR=NSANRFRE/RTMTRESC; ; /* Data Element Derivation
(NSAAVCHT) */; FORMAT NSAAVCHT SCALE4.; LABEL
NSAAVCHT="AVERAGE TOTAL CHARACTERS TRANSMITTED"; NSAAVCHT
= .; NSATOCTR=SUM(NSANRCBS,NSANRTBS,NSANRCBR,NSANRTBR); IF
RTMTRESC NE 0 THEN NSAAVCHT=NSATOCTR/RTMTRESC; ; /* Data
Element Derivation (NSAAVPIU) */; FORMAT NSAAVPIU SCALE4.;
LABEL NSAAVPIU="AVERAGE PIUS PER/RESPONSE"; NSAAVPIU = .;
NSANRPIU=SUM(NSANRTPR,NSANRTPS,NSANRCPR,NSANRCPS); IF
RTMTRESC GT 0 THEN NSAAVPIU=NSANRPIU/RTMTRESC; ; /* Data
Element Derivation (RTMNRNR) */; FORMAT RTMNRNR SCALE4.;
LABEL RTMNRNR="NUMBER OF RESPONSES NOT IN RANGE";
RTMNRNR = .; RTMNRNR=(RTMTRESC-RTMNRROM); ;

```

SNTLD6/SNTLD7

```

/* Data Element Derivation (DATE) */;
FORMAT DATE DATE7.;
LABEL DATE="Date Selection Field";
DATE = DATEPART(ENDTS);
;
/* Data Element Derivation (TIME) */;
FORMAT TIME TIME11.2;
LABEL TIME="Time Selection Field";
TIME = TIMEPART(ENDTS);
;
/* Data Element Derivation (DATA) */;
LENGTH DATA $15;
FORMAT DATA $CHAR15.;
LABEL DATA="DATA RANGE";
DATA = ' ';
/* SAS System Statements(Derive vars & data select) */;
RETAIN DATEA DATEB;
LENGTH DATEA DATEB 4.;
DATEA = MIN(DATEA,STARTTS);
DATEB=MAX(DATEB,ENDTS);
IF _EOF_ THEN DO;
    DATEA=DATEPART(DATEA);
    DATEB=DATEPART(DATEB);
    SUBSTR(DATA,1,7)=PUT(DATEA,DATE7.);

```

```
        SUBSTR(DATA,8,1)='- ' ;
        SUBSTR(DATA,9,7)=PUT(DATEB,DATE7.);
        CALL SYMPUT('S',DATA);
        %GLOBAL S;
        DROP DATEA DATEB;
    END;
    /* Data Summarization */
    %MACRO NEGATE;
        DATA=SYMGET('S');
    %MEND NEGATE;
;
    /* Data Element Derivation (CURRENT, &C) */;
    FORMAT CURRENT WEEKDATE15.;
    LABEL CURRENT="CURRENT DATE";
    CURRENT = TODAY();
    C=PUT(CURRENT,WEEKDATE15.);
    C=COMPRESS(C) ;
    CALL SYMPUT('C',PUT(C,$CHAR12.));
    %GLOBAL C;
;
    /* Data Element Derivation (IQ, &I) */;
    LENGTH IQ $8;
    FORMAT IQ $CHAR8.;
    LABEL IQ="Inquire Name";
    IQ = ' ' ;
    SUBSTR(IQ,1,1)='(' ;
    SUBSTR(IQ,2,6)=SYMGET('INQINAME');
    SUBSTR(IQ,8,1)=') ' ;
    CALL SYMPUT('I',PUT(IQ,$CHAR8.));
    %GLOBAL I;
;
    /* Data Element Derivation (OBJECTIV) */;
    LENGTH OBJECTIV $12;
    FORMAT OBJECTIV $CHAR12.;
    LABEL OBJECTIV="X PERCENT OF RESPONSE WITHIN XX SECONDS";
    OBJECTIV = ' . ' ;
    IF LSYPCOBJ GE 0 OR LSYROBTM GE 0 THEN DO;
        SUBSTR(OBJECTIV,1,3)=PUT(LSYPCOBJ,3.);
        SUBSTR(OBJECTIV,4,4)='% < ' ;
        SUBSTR(OBJECTIV,8,5)=PUT(LSYROBTM,4.1);
    END;
;
    /* Data Element Derivation (RANKELEM) */;
    FORMAT RANKELEM 8.;
    LABEL RANKELEM="&RL";
    RANKELEM = &RANKELEM;
;
    /* Data Element Derivation (RANKLBL) */;
    LENGTH RANKLBL $40;
```

```

FORMAT RANKLBL $CHAR40.;
LABEL RANKLBL="LABEL OF RANKING ELEMENT";
RANKLBL = SYMGET('RL');
;
/* Data Element Derivation (LSYPCOBS) */;
LENGTH LSYPCOBS $4;
FORMAT LSYPCOBS $CHAR4.;
LABEL LSYPCOBS="% MET OF SAMPLED";
LSYPCOBS = ' . ';
IF LSYPCOBM GE 0 THEN DO;
SUBSTR(LSYPCOBS,1,3)=PUT(LSYPCOBM,3.);
SUBSTR(LSYPCOBS,4,1)='%';
END;
;
/* Data Element Derivation (LSYPCOBT) */;
LENGTH LSYPCOBT $4;
FORMAT LSYPCOBT $CHAR4.;
LABEL LSYPCOBT="% MET OF TOTAL";
LSYPCOBT = ' . ';
IF LSYPCTR4 GE 0 THEN DO;
SUBSTR(LSYPCOBT,1,3)=PUT(LSYPCTR4,3.);
SUBSTR(LSYPCOBT,4,1)='%';
END;
;
/* Data Element Derivation (LSYTRSMN) */;
FORMAT LSYTRSMN SCALE4.;
LABEL LSYTRSMN="TRANSACTIONS PER MINUTE";
LSYTRSMN = .;
DURMINS=(DURATION/60);
IF DURMINS GT 0 THEN LSYTRSMN=LSYTRESC/DURMINS;
;
/* Data Element Derivation (LSYTOTSN) */;
FORMAT LSYTOTSN SCALE4.;
LABEL LSYTOTSN="TOTAL CHARACTERS SENT";
LSYTOTSN = SUM(LSYNRCBS,LSYNRTBS);
;
/* Data Element Derivation (LSYTOTRC) */;
FORMAT LSYTOTRC SCALE4.;
LABEL LSYTOTRC="TOTAL CHARACTERS RECEIVED";
LSYTOTRC = SUM(LSYNRCBR,LSYNRTBR);
;
/* Data Element Derivation (LSYTOTTR) */;
FORMAT LSYTOTTR SCALE4.;
LABEL LSYTOTTR="TOTAL CHARACTERS TRANSMITTED";
LSYTOTTR = SUM(LSYNRCBR,LSYNRTBR,LSYNRCBS,LSYNRTBS);
;
/* Data Element Derivation (LSYAVCHS) */;
FORMAT LSYAVCHS SCALE4.;
LABEL LSYAVCHS="AVERAGE CHARACTERS SENT";

```

```
LSYAVCHS = .;
LSYNRFSR=SUM(LSYNRCBS,LSYNRTBS);
IF LSYTRESC GT 0 THEN LSYAVCHS=LSYNRFSR/LSYTRESC;
;
/* Data Element Derivation (LSYAVCHR) */;
FORMAT LSYAVCHR SCALE4.;
LABEL LSYAVCHR="AVERAGE CHARACTERS RECEIVED";
LSYAVCHR = .;
LSYNRFRE=SUM(LSYNRCBR,LSYNRTBR);
IF LSYTRESC NE 0 THEN LSYAVCHR=LSYNRFRE/LSYTRESC;
;
/* Data Element Derivation (LSYAVCHT) */;
FORMAT LSYAVCHT SCALE4.;
LABEL LSYAVCHT="AVERAGE TOTAL CHARACTERS TRANSMITTED";
LSYAVCHT = .;
LSYTOCTR=SUM(LSYNRCBS,LSYNRTBS,LSYNRCBR,LSYNRTBR);
IF LSYTRESC NE 0 THEN LSYAVCHT=LSYTOCTR/LSYTRESC;
;
/* Data Element Derivation (LSYAVPIU) */;
FORMAT LSYAVPIU SCALE4.;
LABEL LSYAVPIU="AVERAGE PIUS PER/RESPONSE";
LSYAVPIU = .;
LSYNRPIU=SUM(LSYNRTPR,LSYNRTPS,LSYNRCPR,LSYNRCPS);
IF LSYTRESC GT 0 THEN LSYAVPIU=LSYNRPIU/LSYTRESC;
;
/* Data Element Derivation (LSYNRRNR) */;
FORMAT LSYNRNR SCALE4.;
LABEL LSYNRNR="NUMBER OF RESPONSES NOT IN RANGE";
LSYNRRNR = .;
LSYNRRNR=(LSYTRESC-LSYNRROR);
;
```

USAGE CONSIDERATIONS:

All cycles are summarized together as a data range rather than reporting by individual cycle or by year, month, day, and hour as other CA MICS reports do.

1

(SNTLDA) DAILY APPLICATION RANKING BY ZONE																
FIRST 10 APPLICATIONS BY DESCENDING AVERAGE TOTAL RESPONSE TIME																
NETWORK ID: NETWORK1 SYSTEM ID: SYSA DATA RANGE: 23JULyy-01APRyy ZONE: 2																
- IDENTIFICATION -		----- RESPONSE INFORMATION -----										----- WORKLOAD INFORMATION -----				
DURATION(HH:MM) /		AVG	RESPONSE	MISSED	RATE	- % MET OF -		-- TOTAL # --		--- TOTAL CHARS ---		----- AVG CHARS -----		PIUS /		
APPLICATION NAME		RESP	OBJECTIVE	OBJ	/ MIN	SAMP	TOTAL	RESP	SAMPLES	SENT	RECVD	TRANS	SENT	RECVD	TRANS	RESP
=====		=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====
0:00	TVS2	1.65	85% < 5.0	0	2	100%	100%	2	2	0	0	0	0	0	0	0
0:01	H160X	1.48	85% < 5.0	9	5	100%	100%	11	2	0	0	0	0	0	0	0
0:01	H160Q8VC	0.49	85% < 5.0	11	11	100%	100%	12	1	0	0	0	0	0	0	0
0:00	H160Q4VC	0.31	85% < 5.0	7	26	100%	100%	8	1	0	0	0	0	0	0	0
0:00	HA99N	.	.	0	0	.	.	0	1	4	76	80	0	0	0	0
0:00	HA99N	.	.	0	0	.	.	0	13	36	779	815	0	0	0	0
0:00	HD93N	.	.	0	0	.	.	0	1	0	55	55	0	0	0	0
0:00	HD93N002	.	.	0	0	.	.	0	1	0	56	56	0	0	0	0
0:01	H059CSM1	.	.	0	0	.	.	0	102	30K	1K	32K	0	0	0	0
0:00	H059CSM3	.	.	0	0	.	.	0	4	1K	67	1K	0	0	0	0
=====		=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=RTMAVTTM=AVERAGE TOTAL RESPONSE TIME
 RUN-DATE=Wed,Sep3,yy , TIMESpan=DAYS, DBID=8, FILE=NSA/RTM

2

(SNTLDA) DAILY APPLICATION RANKING BY ZONE																
FIRST 10 APPLICATIONS BY DESCENDING AVERAGE TOTAL RESPONSE TIME																
NETWORK ID: NETWORK1 SYSTEM ID: SYSB DATA RANGE: 23JULyy-01APRyy ZONE: 1																
- IDENTIFICATION -		----- RESPONSE INFORMATION -----										----- WORKLOAD INFORMATION -----				
DURATION(HH:MM) /		AVG	RESPONSE	MISSED	RATE	- % MET OF -		-- TOTAL # --		--- TOTAL CHARS ---		----- AVG CHARS -----		PIUS /		
APPLICATION NAME		RESP	OBJECTIVE	OBJ	/ MIN	SAMP	TOTAL	RESP	SAMPLES	SENT	RECVD	TRANS	SENT	RECVD	TRANS	RESP
=====		=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====
0:30	P18IMSB	31.0	95% < 4.0	5	0	0%	40%	5	2	0	0	0	0	0	0	0
0:32	C41TS239	24.2	95% < 4.0	36	1	100%	97%	39	3	28K	946	29K	734	24	758	9
0:05	C41TS221	17.3	95% < 4.0	5	0	0%	80%	5	1	66K	1K	67K	13K	256	13K	81
0:15	C41TS205	11.0	95% < 4.0	23	1	0%	74%	23	1	0	0	0	0	0	0	0
0:45	C41TS138	10.9	95% < 4.0	3	0	67%	80%	5	3	0	0	0	0	0	0	0
0:15	C41TS276	8.86	95% < 4.0	33	2	0%	52%	33	2	12K	1K	13K	364	32	397	7
0:03	C41TS267	8.66	95% < 4.0	12	3	0%	83%	12	1	21K	727	22K	1K	60	1K	24
0:45	C41TS054	8.37	95% < 4.0	43	0	33%	82%	44	3	0	0	0	0	0	0	0
0:45	C41TS068	8.36	95% < 4.0	29	0	33%	80%	30	3	0	0	0	0	0	0	0
1:00	C41TS278	7.41	95% < 4.0	236	3	50%	97%	238	4	0	0	0	0	0	0	0
=====		=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=RTMAVTTM=AVERAGE TOTAL RESPONSE TIME
 RUN-DATE=Wed,Sep3,yy , TIMESpan=DAYS, DBID=8, FILE=NSA/RTM

Figure 3-

3.3.1.1.8 NetView Link Service/Workload Ranking

INTENDED USE:

To rank all or selected links in ascending or descending order based on response times or character traffic volumes. The user chooses the number of links ranked, the order of ranking, and the variable used to rank on. The report provides both response and workload information that can be used to identify links having high traffic volume or response time.

FORMAT:

A 17 column report approximately 132 characters wide. It is best suited for hardcopy review but can be reviewed online. The information is summarized and presented by NETWRKID, SYSID, SLULINK, Data Range, and Zone or Zone by Hour.

INQUIRY ID:

SNTLD8 - Link w/in zone
SNTLD9 - Link w/in hour

DATA SOURCE (File/Timespan):

SNTNLL01 - Days

DATA ELEMENTS USED:

DURATION, SLULINK, NLLAVTTM, NLLTRESC, NLLTRSMN, NLLTOTSN, NLLTSTRC, NLLTOTTR, NLLTCTMN, NLLAVCHS, NLLAVCHR, CURRENT, NLLAVCHT, NLLNRPIS, NLLNRPIS, NLLNRPIT, NLLAVLMN, RANKLBL, NLLAVPIU, NETWRKID, SYSID, DATA, ZONE, DATE, TIME, IQ, RANKELEM

CALCULATIONS:

```
/* Data Element Derivation (DATE) */;
FORMAT DATE DATE7.;
LABEL DATE="Date Selection Field";
DATE = DATEPART(ENDTS);
;
/* Data Element Derivation (TIME) */;
FORMAT TIME TIME11.2;
LABEL TIME="Time Selection Field";
TIME = TIMEPART(ENDTS);
```

```

;
/* Data Element Derivation (DATA) */;
LENGTH DATA $15;
FORMAT DATA $CHAR15.;
LABEL DATA="DATA RANGE";
DATA = ' ';
/* SAS System Statements(Derive vars & data select) */;
RETAIN DATEA DATEB;
LENGTH DATEA DATEB 4.;
IF SLULINK NE ' ' THEN DO;
    DATEA = MIN(DATEA,STARTTS);
    DATEB=MAX(DATEB,ENDTS);
END;
IF _EOF_ THEN DO;
    DATEA=DATEPART(DATEA);
    DATEB=DATEPART(DATEB);
    SUBSTR(DATA,1,7)=PUT(DATEA,DATE7.);
    SUBSTR(DATA,8,1)='- ';
    SUBSTR(DATA,9,7)=PUT(DATEB,DATE7.);
    CALL SYMPUT('S',DATA);
    %GLOBAL S;
    DROP DATEA DATEB;
END;
IF SLULINK NE ' '; /*DROP LOCALLY ATTACHED*/
/* Data Summarization */
%MACRO NEGATE;
    DATA=SYMGET('S');
%MEND NEGATE;
;
/* Data Element Derivation (CURRENT, &C) */;
FORMAT CURRENT WEEKDATE15.;
LABEL CURRENT="CURRENT DATE";
CURRENT = TODAY();
C=PUT(CURRENT,WEEKDATE15.);
C=COMPRESS(C) ;
CALL SYMPUT('C',PUT(C,$CHAR12.));
%GLOBAL C;
;
/* Data Element Derivation (IQ, &I) */;
LENGTH IQ $8;
FORMAT IQ $CHAR8.;
LABEL IQ="Inquire Name";
IQ = ' ';
SUBSTR(IQ,1,1)='(';
SUBSTR(IQ,2,6)=SYMGET('INQINAME');
SUBSTR(IQ,8,1)=')';
CALL SYMPUT('I',PUT(IQ,$CHAR8.));
%GLOBAL I;
;

```

```
/* Data Element Derivation (RANKELEM) */;
FORMAT RANKELEM 8.;
LABEL RANKELEM="&RL";
RANKELEM = &RANKELEM;
;
/* Data Element Derivation (RANKLBL) */;
LENGTH RANKLBL $40;
FORMAT RANKLBL $CHAR40.;
LABEL RANKLBL="LABEL OF RANKING ELEMENT";
RANKLBL = SYMGET('RL');
;
/* Data Element Derivation (NLLTRSMN) */;
FORMAT NLLTRSMN SCALE4.;
LABEL NLLTRSMN="TRANSACTIONS PER MINUTE";
NLLTRSMN = .;
DURMINS=(DURATION/60);
IF DURMINS GT 0 THEN NLLTRSMN = NLLTRESN/DURMINS;
;
/* Data Element Derivation (NLLTOTS) */;
FORMAT NLLTOTS SCALE4.;
LABEL NLLTOTS="TOTAL CHARACTERS SENT";
NLLTOTS = SUM(NLLNRCS,NLLNRTBS);
;
/* Data Element Derivation (NLLTOTRC) */;
FORMAT NLLTOTRC SCALE4.;
LABEL NLLTOTRC="TOTAL CHARACTERS RECEIVED";
NLLTOTRC = SUM(NLLNRCSR,NLLNRTBR);
;
/* Data Element Derivation (NLLTOTTR) */;
FORMAT NLLTOTTR SCALE4.;
LABEL NLLTOTTR="TOTAL CHARACTERS TRANSMITTED";
NLLTOTTR = SUM(NLLNRCSR,NLLNRTBR,NLLNRCS,NLLNRTBS);
;
/* Data Element Derivation (NLLTCTMN) */;
FORMAT NLLTCTMN SCALE4.;
LABEL NLLTCTMN="AVG CHARACTERS TRANSMITTED PER MINUTE";
NLLTCTMN = .;
IF DURATION GT 0 THEN NLLTCTMN =
SUM(NLLNRCSR,NLLNRTBR,NLLNRCS,NLLNRTBS) / (DURATION/60);
;
/* Data Element Derivation (NLLAVCHS) */;
FORMAT NLLAVCHS SCALE4.;
LABEL NLLAVCHS="AVERAGE CHARACTERS SENT";
NLLAVCHS = .;
NLLNRFSR=SUM(NLLNRCS,NLLNRTBS);
IF NLLTRESN GT 0 THEN NLLAVCHS=NLLNRFSR/NLLTRESN;
;
/* Data Element Derivation (NLLAVCHR) */;
FORMAT NLLAVCHR SCALE4.;
```

```

LABEL NLLAVCHR="AVERAGE CHARACTERS RECEIVED";
NLLAVCHR = .;
NLLNRFRE=SUM(NLLNRCBR,NLLNRTBR);
IF NLLTRES NE 0 THEN NLLAVCHR=NLLNRFRE/NLLTRES;
;
/* Data Element Derivation (NLLAVCHT) */;
FORMAT NLLAVCHT SCALE4.;
LABEL NLLAVCHT="AVERAGE TOTAL CHARACTERS TRANSMITTED";
NLLAVCHT = .;
NLLTOCTR=SUM(NLLNRCBS,NLLNRTBS,NLLNRCBR,NLLNRTBR);
IF NLLTRES NE 0 THEN NLLAVCHT=NLLTOCTR/NLLTRES;
;
/* Data Element Derivation (NLLNRPIS) */;
FORMAT NLLNRPIS SCALE4.;
LABEL NLLNRPIS="TOTAL PIUs SENT";
NLLNRPIS = SUM(NLLNRTPS,NLLNRCPS);
;
/* Data Element Derivation (NLLNRPIS) */;
FORMAT NLLNRPIS SCALE4.;
LABEL NLLNRPIS="TOTAL PIUs RECEIVED";
NLLNRPIS = SUM(NLLNRTPR,NLLNRCPR);
;
/* Data Element Derivation (NLLNRPIT) */;
FORMAT NLLNRPIT SCALE4.;
LABEL NLLNRPIT="TOTAL PIUs TRANSMITTED";
NLLNRPIT = SUM(NLLNRTPR,NLLNRTPS,NLLNRCPR,NLLNRCPS);
;
/* Data Element Derivation (NLLAVPIU) */;
FORMAT NLLAVPIU SCALE4.;
LABEL NLLAVPIU="AVERAGE PIUs PER/RESPONSE";
NLLAVPIU = .;
NLLNRPIS=SUM(NLLNRTPR,NLLNRTPS,NLLNRCPR,NLLNRCPS);
IF NLLTRES GT 0 THEN NLLAVPIU=NLLNRPIS/NLLTRES;
;
/* Data Element Derivation (NLLAVPMN) */;
FORMAT NLLAVPMN SCALE4.;
LABEL NLLAVPMN="AVG PIUs TRANSMITTED PER MINUTE";
NLLAVPMN = .;
TOTPIUS=SUM(NLLNRTPR,NLLNRTPS,NLLNRCPR,NLLNRCPS);
DURMINS=(DURATION/60);
IF DURMINS GT 0 THEN NLLAVPMN=TOTPIUS/DURMINS;
;

```

USAGE CONSIDERATIONS:

All cycles are summarized together as a data range rather

than reporting by individual cycle or by year, month, day,
and hour as other CA MICS reports do.

1

```
(SNTLD8) DAILY LINK RANKING BY ZONE
FIRST 10 LINKS BY DESCENDING AVERAGE TOTAL RESPONSE TIME
NETWORK ID: NETWORK1    SYSTEM ID: SYSA    DATA RANGE: 22JULyy-01APRyy    ZONE: 2
|-----IDENTIFICATION-----| |-----RESP INFORMATION-----| |-----WORKLOAD INFORMATION-----|
|DURATION(HH:MM) / | |AVG  TOTAL  RATE  | |----- TOTAL CHARS -----| |----- AVG CHARS -----| |----- TOTAL PIUS ---| |----- PIUS PER ---|
|LINK NAME | |RESP  RESPS  / MIN | |SENT  RECVD  TRANS  / MIM| |SENT  RECVD  TRANS | |SENT  RECVD  TRANS| | / MIN  / RESP |
|=====| |=====| |=====| |=====| |=====| |=====| |=====| |=====|
5:00 L063V378  1.67    4    0    63    1K    1K    5    15    421    437    21    21    42    0    10
0:00 L141016   1.65    2    2    0     0     0     0     0     0     0     0     0     0     0     0
5:01 L491V874   1.37    7    0   177    4K    5K   17   25   709   734   59   59   118    0   16
5:01 L071V039   0.49   12    0   186    4K    5K   17   15   413   428   62   62   124    0   10
5:00 L083V198   0.31    8    0    42    1K    1K    4     5   147   152   14   14    28    0    3
0:45 N002NPAL   .        0    0    2   18K   18K  413    0    0     0     1   48   49    1    0
0:30 N003NPAL   .        0    0    0    3K    3K  101    0    0     0     0   21   21    0    0
0:45 N004NPAL   .        0    0    2   23K   23K  532    0    0     0     1   56   57    1    0
0:45 N005NPAL   .        0    0    0   22K   22K  495    0    0     0     0  143  143    3    0
0:45 N006NPAL   .        0    0    0    5K    5K  120    0    0     0     0   38   38    0    0
```

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NLAVTTM=AVERAGE TOTAL RESPONSE TIME
RUN-DATE=Wed,Sep3,yy , TIMESpan=DAYS, DBID=8, FILE=NULL

2

(SNTLD8) DAILY LINK RANKING BY ZONE

FIRST 10 LINKS BY DESCENDING AVERAGE TOTAL RESPONSE TIME

NETWORK ID: NETWORK1 SYSTEM ID: SYSB DATA RANGE: 22JULyy-01APRyy ZONE: 1

-IDENTIFICATION-- - RESP INFORMATION - -----				WORKLOAD INFORMATION ----- -----											
DURATION(HH:MM) /		AVG	TOTAL	RATE	TOTAL CHARS			AVG CHARS			TOTAL PIUS			PIUS PER	
LINK NAME		RESP	RESPS	/ MIN	SENT	RECVD	TRANS	/ MIN	SENT	RECVD	TRANS	SENT	RECVD	TRANS	/ MIN / RESP
67:02	CC000067	7.73	60	0	46K	2K	49K	12	782	43	826	169	243	412	0 6
50:55	CC000002	3.97	1K	0	161K	9K	170K	55	109	6	115	874	1K	1K	0 1
10:36	CC000096	2.97	547	0	30K	2K	32K	51	55	4	60	107	126	233	0 0
12:58	CC000035	2.78	685	0	0	0	0	0	0	0	0	0	0	0	0 0
46:10	0C14	2.76	1K	0	196K	23K	219K	79	195	22	217	766	1K	2K	0 2
16:28	0A15	2.68	386	0	137K	75K	212K	214	355	194	550	606	1K	1K	1 4
77:42	0A16	2.48	1K	0	440K	14K	455K	97	307	10	317	1K	1K	2K	0 1
1:45	0A26	2.44	278	2	0	0	0	0	0	0	0	0	0	0	0 0
17:23	0A19	2.39	908	0	35K	5K	40K	39	38	6	45	93	146	239	0 0
20:27	0C10	2.33	424	0	54K	14	54K	44	127	0	127	131	131	262	0 0

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NLLAVTTM=AVERAGE TOTAL RESPONSE TIME

RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NLL

Figure 3-

3.3.1.1.9 NetView PCLASS Service/Workload Ranking

INTENDED USE:

To rank all or selected NetView performance classes in ascending or descending order based on response times or character traffic volumes. The user chooses the number of performance classes ranked, the order of ranking, and the variable used to rank on. The report provides both response and workload information that can be used to identify performance classes having high traffic volume or response times.

FORMAT:

A 17 column report approximately 132 characters wide. It is best suited for hardcopy review but can be reviewed online. The information is summarized and presented by NETWRKID, SYSID, PERFLSS, Data Range, and Zone or Zone by Hour.

INQUIRY ID:

SNTLDC - PCLASS w/in zone
SNTLDD - PCLASS w/in hour

DATA SOURCE (File/Timespan):

NVSNSA/NVSRTM - Days

DATA ELEMENTS USED:

DURATION, SNTACT4, RTMAVTTM, OBJECTIV, RTMNRNR, RTMTRSMN,
RTMPCOBS, RTMPCOBT, RTMTRESC, SAMPLES, NSATOTSN, NSATOTRC,
NSATOTTR, NSAACVHS, NSAAVCHR, NSAAVCHT, NSAAVPIU, SYSID,
NETWRKID, DATA, ZONE, RANKELEM, RANKLBL, CURRENT, DATE,
TIME, IQ

CALCULATIONS:

```
/* Data Element Derivation (DATE) */;
FORMAT DATE DATE7.;
LABEL DATE="Date Selection Field";
DATE = DATEPART(ENDTS);
;
/* Data Element Derivation (TIME) */;
FORMAT TIME TIME11.2;
LABEL TIME="Time Selection Field";
TIME = TIMEPART(ENDTS);
;
```



```

/* Data Element Derivation (DATA) */;
LENGTH DATA $15;
FORMAT DATA $CHAR15.;
LABEL DATA="DATA RANGE";
DATA = ' ';
/* SAS System Statements (Load DATA Variable) */;
RETAIN DATEA DATEB;
LENGTH DATEA DATEB 4.;
IF SESTYPE =:'LU-LU' THEN DO;
    DATEA = MIN(DATEA,STARTTS);
    DATEB = MAX(DATEB,ENDTS);
END;
IF _EOF_ THEN DO;
    DATEA=DATEPART(DATEA);
    DATEB=DATEPART(DATEB);
    SUBSTR(DATA,1,7)=PUT(DATEA,DATE7.);
    SUBSTR(DATA,8,1)='- ';
    SUBSTR(DATA,9,7)=PUT(DATEB,DATE7.);
    DROP DATEA DATEB;
    CALL SYMPUT('S',DATA);
    %GLOBAL S;
END;
IF SESTYPE =:'LU-LU';
/* Data Summarization */
%MACRO NEGATE;
    DATA=SYMGET('S');
%MEND NEGATE;
;
/* Data Element Derivation (IQ, &I) */;
LENGTH IQ $8;
FORMAT IQ $CHAR8.;
LABEL IQ="INQUIRE NAME";
IQ = ' ';
SUBSTR(IQ,1,1)='(';
SUBSTR(IQ,2,6)=SYMGET('INQINAME');
SUBSTR(IQ,8,1)=')';
CALL SYMPUT('I',PUT(IQ,$CHAR8.));
%GLOBAL I;
;
/* Data Element Derivation (CURRENT, &C) */;
FORMAT CURRENT WEEKDATE15.;
LABEL CURRENT="CURRENT DATE";
CURRENT = TODAY();
C=PUT(CURRENT,WEEKDATE15.);
C=COMPRESS(C) ;
CALL SYMPUT('C',PUT(C,$CHAR12.));
%GLOBAL C;
;
/* Data Element Derivation (OBJECTIV) */;

```

```
LENGTH OBJECTIV $12;
FORMAT OBJECTIV $CHAR12.;
LABEL OBJECTIV="X PERCENT OF RESPONSE WITHIN XX SECONDS";
OBJECTIV = ' . ';
IF RTMPCOBJ GE 0 OR RTMROBTM GE 0 THEN DO;
SUBSTR(OBJECTIV,1,3)=PUT(RTMPCOBJ,3.);
SUBSTR(OBJECTIV,4,4)='% < ';
SUBSTR(OBJECTIV,8,5)=PUT(RTMROBTM,4.1);
END;
;
/* Data Element Derivation (RANKELEM) */;
FORMAT RANKELEM 8.;
LABEL RANKELEM="&RL";
RANKELEM = &RANKELEM;
;
/* Data Element Derivation (RANKLBL) */;
LENGTH RANKLBL $40;
FORMAT RANKLBL $CHAR40.;
LABEL RANKLBL="LABEL OF RANKING ELEMENT";
RANKLBL = SYMGET('RL');
;
/* Data Element Derivation (RTMPCOBS) */;
LENGTH RTMPCOBS $4;
FORMAT RTMPCOBS $CHAR4.;
LABEL RTMPCOBS="% MET OF SAMPLED";
RTMPCOBS = ' . ';
IF RTMPCOBM GE 0 THEN DO;
SUBSTR(RTMPCOBS,1,3)=PUT(RTMPCOBM,3.);
SUBSTR(RTMPCOBS,4,1)='%';
END;
;
/* Data Element Derivation (RTMPCOBT) */;
LENGTH RTMPCOBT $4;
FORMAT RTMPCOBT $CHAR4.;
LABEL RTMPCOBT="% MET OF TOTAL";
RTMPCOBT = ' . ';
IF RTMPCTR4 GE 0 THEN DO;
SUBSTR(RTMPCOBT,1,3)=PUT(RTMPCTR4,3.);
SUBSTR(RTMPCOBT,4,1)='%';
END;
;
/* Data Element Derivation (RTMTRSMN) */;
FORMAT RTMTRSMN SCALE4.;
LABEL RTMTRSMN="TRANSACTIONS PER MINUTE";
RTMTRSMN = .;
DURMINS=(DURATION/60);
IF DURMINS GT 0 THEN
RTMTRSMN=RTMTRESC/DURMINS;
;
```

```

/* Data Element Derivation (NSATOTSN) */;
FORMAT NSATOTSN SCALE4.;
LABEL NSATOTSN="TOTAL CHARACTERS SENT";
NSATOTSN = SUM(NSANRCBS,NSANRTBS);
;
/* Data Element Derivation (NSATOTRC) */;
FORMAT NSATOTRC SCALE4.;
LABEL NSATOTRC="TOTAL CHARACTERS RECEIVED";
NSATOTRC = SUM(NSANRCBR,NSANRTBR);
;
/* Data Element Derivation (NSATOTTR) */;
FORMAT NSATOTTR SCALE4.;
LABEL NSATOTTR="TOTAL CHARACTERS TRANSMITTED";
NSATOTTR = SUM(NSANRCBR,NSANRTBR,NSANRCBS,NSANRTBS);
;
/* Data Element Derivation (NSAAVCHS) */;
FORMAT NSAAVCHS SCALE4.;
LABEL NSAAVCHS="AVERAGE CHARACTERS SENT";
NSAAVCHS = .;
NSANRFSR=SUM(NSANRCBS,NSANRTBS);
IF RTMTRESC GT 0 THEN NSAAVCHS=NSANRFSR/RTMTRESC;
;
/* Data Element Derivation (NSAAVCHR) */;
FORMAT NSAAVCHR SCALE4.;
LABEL NSAAVCHR="AVERAGE CHARACTERS RECEIVED";
NSAAVCHR = .;
NSANRFRE=SUM(NSANRCBR,NSANRTBR);
IF RTMTRESC NE 0 THEN NSAAVCHR=NSANRFRE/RTMTRESC;
;
/* Data Element Derivation (NSAAVCHT) */;
FORMAT NSAAVCHT SCALE4.;
LABEL NSAAVCHT="AVERAGE TOTAL CHARACTERS TRANSMITTED";
NSAAVCHT = .;
NSATOCTR=SUM(NSANRCBS,NSANRTBS,NSANRCBR,NSANRTBR);
IF RTMTRESC NE 0 THEN NSAAVCHT=NSATOCTR/RTMTRESC;
;
/* Data Element Derivation (NSAAVPIU) */;
FORMAT NSAAVPIU SCALE4.;
LABEL NSAAVPIU="AVERAGE PIUS PER/RESPONSE";
NSAAVPIU = .;
NSANRPIU=SUM(NSANRTPR,NSANRTPS,NSANRCPR,NSANRCPS);
IF RTMTRESC GT 0 THEN NSAAVPIU=NSANRPIU/RTMTRESC;
;
/* Data Element Derivation (RTMNRNR) */;
FORMAT RTMNRNR SCALE4.;
LABEL RTMNRNR="NUMBER OF RESPONSES NOT IN RANGE";
RTMNRNR = .;
RTMNRNR=(RTMTRESC-RTMNRROM);
;

```

USAGE CONSIDERATIONS:

All cycles are summarized together as a data range rather than reporting by individual cycle or by year, month, day, and hour as other CA MICS reports do.

1

(SNTLDC) DAILY PERFORMANCE CLASS RANKING BY ZONE
FIRST 10 PERFORMANCE CLASSES BY DESCENDING AVERAGE TOTAL RESPONSE TIME
NETWORK ID: NETWORK1 SYSTEM ID: SYSA DATA RANGE: 23JULyy-01APRyy ZONE: 2

-IDENTIFICATION--		RESPONSE INFORMATION										WORKLOAD INFORMATION						
DURATION(HH:MM) /		AVG	RESPONSE	MISSED	RATE	- % MET OF -		TOTAL #		TOTAL CHARS		AVG CHARS			PIUS			
PERFORMANCE CLASS	RESP	OBJECTIVE	OBJ	/ MIN	SAMP	TOTAL	RESP	SAMPLES	SENT	RECVD	TRANS	SENT	RECVD	TRANS	RESP			
0:04 DEFAULT	0.85	85% < 5.0	27	8	100%	100%	33	6	44K	7M	7M	1K	234K	235K	686			
0:00	.	.	0	0	.	.	0	1	4	76	80	0	0	0	0			

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=RTMAVTTM=AVERAGE TOTAL RESPONSE TIME
RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NSA/RTM

2

(SNTLDC) DAILY PERFORMANCE CLASS RANKING BY ZONE																	
FIRST 10 PERFORMANCE CLASSES BY DESCENDING AVERAGE TOTAL RESPONSE TIME																	
NETWORK ID: NETWORK1			SYSTEM ID: SYSB			DATA RANGE: 23JULyy-01APRyy					ZONE: 1						
-IDENTIFICATION--		RESPONSE INFORMATION							WORKLOAD INFORMATION								
DURATION(HH:MM)	/	AVG	RESPONSE	MISSED	RATE	-	% MET OF	-	TOTAL #	-	TOTAL CHARS	-	AVG CHARS	-	PIUS	/	
PERFORMANCE CLASS		RESP	OBJECTIVE	OBJ	/ MIN		SAMP	TOTAL	RESP	SAMPLES	SENT	RECVD	TRANS	SENT	RECVD	TRANS	
0:30	BIMS	31.0	95% < 4.0	5	0	0%	40%	5	2	0	0	0	0	0	0	0	
5:23	TIMS	4.21	95% < 4.0	160	0	46%	94%	172	26	58K	56K	114K	339	326	666	3	
3:09	RIMS	2.71	95% < 4.0	179	1	78%	99%	193	18	52K	68K	120K	271	353	624	3	
92:13	LIMS	2.23	95% < 4.0	4K	0	70%	99%	4K	384	481K	201K	683K	97	40	137	0	
12:20	TCC	2.11	95% < 4.0	710	1	72%	98%	754	61	1M	636K	1M	1K	844	2K	8	
53:42	BDTSO	1.81	95% < 4.0	12K	3	55%	98%	12K	264	15M	1M	16M	1K	93	1K	9	
34:09	SUPER	1.78	95% < 4.0	3K	1	55%	98%	3K	139	1M	26K	1M	358	6	365	1	
1:15	PDTSO	1.56	95% < 4.0	181	2	40%	96%	183	5	277K	2K	279K	1K	13	1K	5	
1:49	ALLOTH	0.94	95% < 5.0	289	2	82%	100%	298	11	6M	1M	8M	22K	4K	27K	99	
2:17	AIMS	0.94	95% < 4.0	151	1	100%	99%	161	10	10K	2K	13K	65	16	81	0	

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=RTMAVTTM=AVERAGE TOTAL RESPONSE TIME
RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NSA/RTM

Figure 3-

3.3.1.1.10 NPM Application Service/Workload Ranking

INTENDED USE:

To rank all or selected applications in ascending or descending order based on response times or character traffic volumes. The user chooses the number of applications ranked, the order of ranking, and the variable used to rank on. The report provides both response and workload information that can be used to identify applications having high traffic volumes or response times.

FORMAT:

A 17 column report approximately 132 characters wide. It is best suited for hardcopy review but can be reviewed online. The information is summarized and presented by NETWRKID, SYSID, PLU, Data Range, and Zone or Zone by Hour.

INQUIRY ID:

SNTLD0 - Application w/in zone
SNTLD1 - Application w/in hour

DATA SOURCE (File/Timespan):

SNTPSY - Days

DATA ELEMENTS USED:

DURATION, PLU, PSYAVTTM, PSYAVHTM, PSYAVNTM, PSYNRTRE,
RANGE, PSYTRESC, PSYTRSMN, PSYPCNTM, PSYTOTSN, PSTTOTRC,
PSYTOTTR, PSYAVCHS, PSYAVCHR, PSYAVCHT, PSYAVPIU, TIME,
NETWRKID, SYSID, DATA, ZONE, RANKELEM, RANKLBL, DATE,
CURRENT, IQ

CALCULATIONS:

```
/* Data Element Derivation (DATE) */;  
FORMAT DATE DATE7.;  
LABEL DATE="Date Selection Field";  
DATE = DATEPART(ENDTS);  
;  
/* Data Element Derivation (TIME) */;  
FORMAT TIME TIME11.2;  
LABEL TIME="Time Selection Field";  
TIME = TIMEPART(ENDTS);
```

```

;
/* Data Element Derivation (DATA) */;
LENGTH DATA $15;
FORMAT DATA $CHAR15.;
LABEL DATA="DATA RANGE";
DATA = ' ';
/* SAS System Statements (Derived vars & data select) */;
RETAIN DATEA DATEB;
LENGTH DATEA DATEB 4.;
DATEA = MIN(DATEA,STARTTS);
DATEB=MAX(DATEB,ENDTS);
IF _EOF_ THEN DO;
    DATEA=DATEPART(DATEA);
    DATEB=DATEPART(DATEB);
    SUBSTR(DATA,1,7)=PUT(DATEA,DATE7.);
    SUBSTR(DATA,8,1)='- ';
    SUBSTR(DATA,9,7)=PUT(DATEB,DATE7.);
    CALL SYMPUT('S',DATA);
    %GLOBAL S;
    DROP DATEA DATEB;
END;
/* Data Summarization */
%MACRO NEGATE;
    DATA=SYMGET('S');
%MEND NEGATE;
;
/* Data Element Derivation (RANGE) */;
LENGTH RANGE $7;
FORMAT RANGE $CHAR7.;
LABEL RANGE="LOW-HI TOTAL RESPONSE THRESHOLD";
RANGE = ' ';
SUBSTR(RANGE,1,3)=PUT(NPMLTOT,3.1);
SUBSTR(RANGE,4,1)='- ';
SUBSTR(RANGE,5,3)=PUT(NPMHITOT,3.1);
;
/* Data Element Derivation (CURRENT, &C) */;
FORMAT CURRENT WEEKDATE15.;
LABEL CURRENT="CURRENT DATE";
CURRENT = TODAY();
C=PUT(CURRENT,WEEKDATE15.);
C=COMPRESS(C) ;
CALL SYMPUT('C',PUT(C,$CHAR12.));
%GLOBAL C;
;
/* Data Element Derivation (IQ, &I) */;
LENGTH IQ $8;
FORMAT IQ $CHAR8.;
LABEL IQ="Inquire Name";
IQ = ' ';

```

```
SUBSTR(IQ,1,1)='(';
SUBSTR(IQ,2,6)=SYMGET('INQINAME');
SUBSTR(IQ,8,1)=')';
CALL SYMPUT('I',PUT(IQ,$CHAR8.));
%GLOBAL I;
;
/* Data Element Derivation (RANKELEM) */;
FORMAT RANKELEM 8.;
LABEL RANKELEM="&RL";
RANKELEM = &RANKELEM;
;
/* Data Element Derivation (RANKLBL) */;
LENGTH RANKLBL $40;
FORMAT RANKLBL $CHAR40.;
LABEL RANKLBL="LABEL OF RANKING ELEMENT";
RANKLBL = SYMGET('RL');
;
/* Data Element Derivation (PSYPCNTM) */;
LENGTH PSYPCNTM $6;
FORMAT PSYPCNTM $CHAR6.;
LABEL PSYPCNTM="% Responses With Network Time";
PSYPCNTM = '    %';
PCTTNETM=(100.0-PSYPCNTM);
SUBSTR(PSYPCNTM,1,5)=PUT(PCTTNETM,5.2);
IF PCTTNETM = . THEN SUBSTR(PSYPCNTM,6,1)=' ';
;
/* Data Element Derivation (DURATION, elapsed time) */;
FORMAT DURATION TIME5.2;
LABEL DURATION="ENDTS - STARTTS";
DURATION = ENDTS-STARTTS;
;
/* Data Element Derivation (PSYTRSMN) */;
FORMAT PSYTRSMN SCALE4.;
LABEL PSYTRSMN="Transactions Per Minute";
PSYTRSMN = .;
DURMINS=(DURATION/60);
IF DURMINS GT 0 THEN PSYTRSMN=PSYTRSMN/DURMINS;
;
/* Data Element Derivation (PSYTOTSN) */;
FORMAT PSYTOTSN 4.;
LABEL PSYTOTSN="Total Characters Sent";
PSYTOTSN = SUM(PSYNRFMS,PSYNRNFS);
;
/* Data Element Derivation (PSYTOTRC) */;
FORMAT PSYTOTRC 4.;
LABEL PSYTOTRC="Total Characters Received";
PSYTOTRC = SUM(PSYNRFMR,PSYNRNFR);
;
/* Data Element Derivation (PSYTOTTR) */;
```



```

FORMAT PSYTOTTR 4.;
LABEL PSYTOTTR="Total Characters Transmitted";
PSYTOTTR = SUM(PSYNRFMR,PSYNRNFR,PSYNRFMS,PSYNRNFS);
;
/* Data Element Derivation (PSYAVCHS) */;
FORMAT PSYAVCHS 4.;
LABEL PSYAVCHS="AVERAGE CHARACTERS SENT";
PSYAVCHS = .;
PSYNRFSR=SUM(PSYNRFMS,PSYNRNFS);
IF PSYTRESC GT 0 THEN PSYAVCHS=PSYNRFSR/PSYTRESC;
;
/* Data Element Derivation (PSYAVCHR) */;
FORMAT PSYAVCHR 4.;
LABEL PSYAVCHR="AVERAGE CHARACTERS RECEIVED";
PSYAVCHR = .;
PSYNRFRE=SUM(PSYNRFMR,PSYNRNFR);
IF PSYTRESC NE 0 THEN PSYAVCHR=PSYNRFRE/PSYTRESC;
;
/* Data Element Derivation (PSYAVCHT) */;
FORMAT PSYAVCHT 4.;
LABEL PSYAVCHT="AVERAGE TOTAL CHARACTERS TRANSMITTED";
PSYAVCHT = .;
PSYTOCTR=SUM(PSYNRFMR,PSYNRNFR,PSYNRFMS,PSYNRNFS);
IF PSYTRESC NE 0 THEN PSYAVCHT=PSYTOCTR/PSYTRESC;
;
/* Data Element Derivation (PSYAVPIU) */;
FORMAT PSYAVPIU SCALE4.;
LABEL PSYAVPIU="AVERAGE PIUS PER/RESPONSE";
PSYAVPIU = .;
PSYNRPIU=SUM(PSYNRPFS,PSYNRPFR);
IF PSYTRESC GT 0 THEN PSYAVPIU=PSYNRPIU/PSYTRESC;
;

```

USAGE CONSIDERATIONS:

All cycles are summarized together as a data range rather than reporting by individual cycle or by year, month, day, and hour as other CA MICS reports do.

1

(SNTLD0) DAILY NPM APPLICATION RANKING BY ZONE

FIRST 10 APPLICATIONS BY DESCENDING AVERAGE TOTAL RESPONSE TIME

NETWORK ID: NETWORK1 SYSTEM ID: SYS1 DATA RANGE: 040CTyy-040CTyy ZONE: 1

-IDENTIFICATION--		----- RESPONSE INFORMATION -----					----- WORKLOAD INFORMATION -----									
ELAPSED(HH:MM) /		---- AVG TIME ----			NOT IN	TOTAL	RATE	% WITH	--- TOTAL CHARS ---			----- AVG CHARS -----			PIUS /	
APPLICATION NAME		TOTAL	HOST	NET	RANGE	RANGE	RESPS	/ MIN	NET TM	SENT	RECVD	TRANS	SENT	RECVD	TRANS	RESP
0:43	TS00046	4.87	0.94	3.92	2	0.0-5.0	10	0	100.0%	7K	211	7K	710	21	732	3
0:58	DIS05S20	3.70	3.70	0.00	101	0.0-5.0	283	4	0.00%	261K	55K	317K	924	196	1K	3
1:15	TS00025	3.27	1.57	1.69	9	0.0-5.0	67	0	100.0%	57K	1K	59K	862	24	887	2
0:55	TS00020	3.22	1.65	1.57	10	0.0-5.0	78	1	100.0%	87K	1K	89K	1K	20	1K	2
0:54	TS00024	2.74	1.07	1.67	6	0.0-5.0	51	0	100.0%	46K	927	47K	914	18	932	2
0:59	TS00038	2.72	1.44	1.28	29	0.0-5.0	216	3	100.0%	177K	4K	181K	822	19	841	2
0:55	TS00022	2.50	0.78	1.72	0	0.0-5.0	6	0	100.0%	8K	91	8K	1K	15	1K	2
1:02	CHRSDC1	2.50	1.70	0.80	7	0.0-5.0	59	0	100.0%	61K	1K	62K	1K	20	1K	2
1:07	TS00005	2.34	1.07	1.27	4	0.0-5.0	27	0	100.0%	23K	732	23K	853	27	880	2
1:07	VTP03	1.92	0.82	1.09	134	0.0-5.0	3K	48	74.13%	1M	64K	1M	591	19	611	2

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=PSYAVTTM=AVERAGE TOTAL RESPONSE TIME

RUN-DATE=Wed,Sep3,yy, TIMESPAN=DAYS, DBID=8, FILE=PSY

Figure 3-

3.3.1.1.11 NPM Link Service/Workload Ranking

INTENDED USE:

To rank all or selected links in ascending or descending order based on response times or character traffic volumes. The user chooses the number of links ranked, the order of ranking, and the variable used to rank on. The report provides both response and workload information that can be used to identify links having high traffic volume or response time.

FORMAT:

A 17 column report approximately 132 characters wide. It is best suited for hardcopy review but can be reviewed online. The information is summarized and presented by NETWRKID, SYSID, SLULINK, Data Range, and Zone or Zone by Hour.

INQUIRY ID:

SNTLD4 - Link w/in zone
SNTLD5 - Link w/in hour

DATA SOURCE (File/Timespan):

SNTNPL - Days

DATA ELEMENTS USED:

DURATION, SLULINK, NPLAVTTM, NPLAVHTM, NPLAVNTM, NPLNRTRE, RANGE, NPLTRES, NPLTRSMN, NPLPCNTM, NPLTOTSN, NPLTOTRC, NPLTOTTR, NPLAVCHS, NPLAVCHR, NPLAVCHT, NPLAVPIU, DATE, NETWRKID, SYSID, DATA, ZONE, RANKELEM, RANKLBL, CURRENT, TIME, IQ

CALCULATIONS:

```
/* Data Element Derivation (DATE) */;
FORMAT DATE DATE7.;
LABEL DATE="Date Selection Field";
DATE = DATEPART(ENDTS);
;
/* Data Element Derivation (TIME) */;
FORMAT TIME TIME11.2;
LABEL TIME="Time Selection Field";
TIME = TIMEPART(ENDTS);
;
```

```
/* Data Element Derivation (DATA) */;
LENGTH DATA $15;
FORMAT DATA $CHAR15.;
LABEL DATA="DATA RANGE";
DATA = ' ';
/* SAS System Statements(Derive vars & data select) */;
RETAIN DATEA DATEB;
LENGTH DATEA DATEB 4.;
IF SLULINK NE ' ' THEN DO;
    DATEA = MIN(DATEA,STARTTS);
    DATEB=MAX(DATEB,ENDTS);
END;
IF _EOF_ THEN DO;
    DATEA=DATEPART(DATEA);
    DATEB=DATEPART(DATEB);
    SUBSTR(DATA,1,7)=PUT(DATEA,DATE7.);
    SUBSTR(DATA,8,1)='- ';
    SUBSTR(DATA,9,7)=PUT(DATEB,DATE7.);
    CALL SYMPUT('S',DATA);
    %GLOBAL S;
    DROP DATEA DATEB;
END;
IF SLULINK NE ' '; /*DROP LOCALLY ATTACHED*/
/* Data Summarization */
%MACRO NEGATE;
    DATA=SYMGET('S');
%MEND NEGATE;
;
/* Data Element Derivation (RANGE) */;
LENGTH RANGE $7;
FORMAT RANGE $CHAR7.;
LABEL RANGE="LOW-HI TOTAL RESPONSE THRESHOLD";
RANGE = ' ';
SUBSTR(RANGE,1,3)=PUT(NPMLTOT,3.1);
SUBSTR(RANGE,4,1)='- ';
SUBSTR(RANGE,5,3)=PUT(NPMHITOT,3.1);
;
/* Data Element Derivation (CURRENT, &C) */;
FORMAT CURRENT WEEKDATE15.;
LABEL CURRENT="CURRENT DATE";
CURRENT = TODAY();
C=PUT(CURRENT,WEEKDATE15.);
C=COMPRESS(C) ;
CALL SYMPUT('C',PUT(C,$CHAR12.));
%GLOBAL C;
;
/* Data Element Derivation (IQ, &I) */;
LENGTH IQ $8;
FORMAT IQ $CHAR8.;
```

```

LABEL IQ="Inquire Name";
IQ = ' ';
SUBSTR(IQ,1,1)='(';
SUBSTR(IQ,2,6)=SYMGET('INQINAME');
SUBSTR(IQ,8,1)=')';
CALL SYMPUT('I',PUT(IQ,$CHAR8.));
%GLOBAL I;
;
/* Data Element Derivation (RANKELEM) */;
FORMAT RANKELEM 8.;
LABEL RANKELEM="&RL";
RANKELEM = &RANKELEM;
;
/* Data Element Derivation (RANKLBL) */;
LENGTH RANKLBL $40;
FORMAT RANKLBL $CHAR40.;
LABEL RANKLBL="LABEL OF RANKING ELEMENT";
RANKLBL = SYMGET('RL');
;
/* Data Element Derivation (NPLPCNTM) */;
LENGTH NPLPCNTM $6;
FORMAT NPLPCNTM $CHAR6.;
LABEL NPLPCNTM="% Responses With Network Time";
NPLPCNTM = '    %';
PCTTNETM=(100.0-NPLPCNON);
SUBSTR(NPLPCNTM,1,5)=PUT(PCTTNETM,5.2);
IF PCTTNETM = . THEN SUBSTR(NPLPCNTM,6,1)=' ';
;
/* Data Element Derivation (DURATION, elapsed time) */;
FORMAT DURATION TIME5.2;
LABEL DURATION="ENDTS - STARTTS";
DURATION = ENDTS-STARTTS;
;
/* Data Element Derivation (NPLTRSMN) */;
FORMAT NPLTRSMN SCALE4.;
LABEL NPLTRSMN="TRANSACTIONS PER MINUTE";
NPLTRSMN = .;
DURMINS=(DURATION/60);
IF DURMINS GT 0 THEN NPLTRSMN=NPLTRES/DURMINS;
;
/* Data Element Derivation (NPLTOTSN) */;
FORMAT NPLTOTSN 4.;
LABEL NPLTOTSN="TOTAL CHARACTERS SENT";
NPLTOTSN = SUM(NPLNRFMS,NPLNRNFS);
;
/* Data Element Derivation (NPLTOTRC) */;
FORMAT NPLTOTRC 4.;
LABEL NPLTOTRC="TOTAL CHARACTERS RECEIVED";
NPLTOTRC = SUM(NPLNRFMR,NPLNRNFR);

```

```
;
/* Data Element Derivation (NPLTOTTR) */;
FORMAT NPLTOTTR 4.;
LABEL NPLTOTTR="TOTAL CHARACTERS TRANSMITTED";
NPLTOTTR = SUM(NPLNRFMR,NPLNRNFR,NPLNRFMS,NPLNRNFS);
;
/* Data Element Derivation (NPLAVCHS) */;
FORMAT NPLAVCHS 4.;
LABEL NPLAVCHS="AVERAGE CHARACTERS SENT";
NPLAVCHS = .;
NPLNRFMR=SUM(NPLNRFMS,NPLNRNFS);
IF NPLTRES GT 0 THEN NPLAVCHS=NPLNRFMR/NPLTRES;
;
/* Data Element Derivation (NPLAVCHR) */;
FORMAT NPLAVCHR 4.;
LABEL NPLAVCHR="AVERAGE CHARACTERS RECEIVED";
NPLAVCHR = .;
NPLNRFRE=SUM(NPLNRFMR,NPLNRNFR);
IF NPLTRES NE 0 THEN NPLAVCHR=NPLNRFRE/NPLTRES;
;
/* Data Element Derivation (NPLAVCHT) */;
FORMAT NPLAVCHT 4.;
LABEL NPLAVCHT="AVERAGE TOTAL CHARACTERS TRANSMITTED";
NPLAVCHT = .;
NPLTOCTR=SUM(NPLNRFMR,NPLNRNFR,NPLNRFMS,NPLNRNFS);
IF NPLTRES NE 0 THEN NPLAVCHT=NPLTOCTR/NPLTRES;
;
/* Data Element Derivation (NPLAVPIU) */;
FORMAT NPLAVPIU SCALE4.;
LABEL NPLAVPIU="AVERAGE PIUS PER/RESPONSE";
NPLAVPIU = .;
NPLNRPIU=SUM(NPLNRPFMS,NPLNRPFMR);
IF NPLTRES GT 0 THEN NPLAVPIU=NPLNRPIU/NPLTRES;
;
```

USAGE CONSIDERATIONS:

All cycles are summarized together as a data range rather than reporting by individual cycle or by year, month, day, and hour as other CA MICS reports do.

1

(SNTLD4) DAILY NPM LINK RANKING BY ZONE																
FIRST 10 LINKS BY DESCENDING AVERAGE TOTAL RESPONSE TIME																
NETWORK ID: NETWORK1 SYSTEM ID: SYS1 DATA RANGE: 040CTyy-040CTyy ZONE: 1																
----- RESPONSE INFORMATION -----																
----- WORKLOAD INFORMATION -----																

3.3.1.1.12 NPM Application/Link Service/Workload Ranking

INTENDED USE:

To rank all or selected application and link combinations in ascending or descending order based on response times or character traffic volumes. The user chooses the number of applications ranked, the order of ranking, and the variable used to rank on. The report provides both response and workload information that can be used to identify applications by link having high traffic volumes or response times.

FORMAT:

A 17 column report approximately 132 characters wide. It is best suited for hardcopy review but can be reviewed online. The information is summarized and presented by NETWRKID, SYSID, PLU, Range, and Zone or Zone by Hour.

INQUIRY ID:

SNTLDQ - Application/Link w/in zone
SNTLDR - Application/Link w/in hour

DATA SOURCE (File/Timespan):

SNTNPL - Days

DATA ELEMENTS USED:

SLULINK, PLU, NPLAVTTM, NPLAVHTM, NPLAVNTM, NPLNRTRE,
RANGE, NPLTRES, NPLTRSMN, NPLPCNTM, NPLTOTS, NPLTOTR,
NPLTOTTR, NPLAVCHS, NPLAVCHR, NPLAVCHT, NPLAVPIU, RANKLBL,
NETWRKID, SYSID, DATA, ZONE, DATE, TIME, CURRENT, IQ,
RANKELEM

CALCULATIONS:

```
/* Data Element Derivation (DATE) */;
FORMAT DATE DATE7.;
LABEL DATE="Date Selection Field";
DATE = DATEPART(ENDTS);
;
/* Data Element Derivation (TIME) */;
FORMAT TIME TIME11.2;
LABEL TIME="Time Selection Field";
TIME = TIMEPART(ENDTS);
;
```



```

/* Data Element Derivation (DATA) */;
LENGTH DATA $15;
FORMAT DATA $CHAR15.;
LABEL DATA="DATA RANGE";
DATA = ' ';
/* SAS System Statements(Derive vars & data select) */;
RETAIN DATEA DATEB;
LENGTH DATEA DATEB 4.;
IF SLULINK NE ' ' THEN DO;
    DATEA = MIN(DATEA,STARTTS);
    DATEB=MAX(DATEB,ENDTS);
END;
IF _EOF_ THEN DO;
    DATEA=DATEPART(DATEA);
    DATEB=DATEPART(DATEB);
    SUBSTR(DATA,1,7)=PUT(DATEA,DATE7.);
    SUBSTR(DATA,8,1)='- ';
    SUBSTR(DATA,9,7)=PUT(DATEB,DATE7.);
    CALL SYMPUT('S',DATA);
    %GLOBAL S;
    DROP DATEA DATEB;
END;
IF SLULINK NE ' '; /*DROP LOCALLY ATTACHED*/
/* Data Summarization */
%MACRO NEGATE;
    DATA=SYMGET('S');
%MEND NEGATE;
;
/* Data Element Derivation (RANGE) */;
LENGTH RANGE $7;
FORMAT RANGE $CHAR7.;
LABEL RANGE="LOW-HI TOTAL RESPONSE THRESHOLD";
RANGE = ' ';
SUBSTR(RANGE,1,3)=PUT(NPMLTOT,3.1);
SUBSTR(RANGE,4,1)='- ';
SUBSTR(RANGE,5,3)=PUT(NPMHITOT,3.1);
;
/* Data Element Derivation (CURRENT, &C) */;
FORMAT CURRENT WEEKDATE15.;
LABEL CURRENT="CURRENT DATE";
CURRENT = TODAY();
C=PUT(CURRENT,WEEKDATE15.);
C=COMPRESS(C) ;
CALL SYMPUT('C',PUT(C,$CHAR12.));
%GLOBAL C;
;
/* Data Element Derivation (IQ, &I) */;
LENGTH IQ $8;
FORMAT IQ $CHAR8.;

```

```

LABEL IQ="Inquire Name";
IQ = ' ';
SUBSTR(IQ,1,1)='(';
SUBSTR(IQ,2,6)=SYMGET('INQINAME');
SUBSTR(IQ,8,1)=')';
CALL SYMPUT('I',PUT(IQ,$CHAR8.));
%GLOBAL I;
;
/* Data Element Derivation (RANKELEM) */;
FORMAT RANKELEM 8.;
LABEL RANKELEM="&RL";
RANKELEM = &RANKELEM;
;
/* Data Element Derivation (RANKLBL) */;
LENGTH RANKLBL $40;
FORMAT RANKLBL $CHAR40.;
LABEL RANKLBL="LABEL OF RANKING ELEMENT";
RANKLBL = SYMGET('RL');
;
/* Data Element Derivation (NPLPCNTM) */;
LENGTH NPLPCNTM $6;
FORMAT NPLPCNTM $CHAR6.;
LABEL NPLPCNTM="% Responses With Network Time";
NPLPCNTM = '    %';
PCTTNETM=(100.0-NPLPCNON);
SUBSTR(NPLPCNTM,1,5)=PUT(PCTTNETM,5.2);
IF PCTTNETM = . THEN SUBSTR(NPLPCNTM,6,1)=' ';
;
/* Data Element Derivation (DURATION, elapsed time) */;
FORMAT DURATION TIME5.2;
LABEL DURATION="ENDTS - STARTTS";
DURATION = ENDTS-STARTTS;
;
/* Data Element Derivation (NPLTRSMN) */;
FORMAT NPLTRSMN 4.2;
LABEL NPLTRSMN="Transactions Per Minute";
NPLTRSMN = .;
DURMINS=(DURATION/60);
IF DURMINS GT 0 THEN NPLTRSMN=NPLTRESC/DURMINS;
;
/* Data Element Derivation (NPLTOTSN) */;
FORMAT NPLTOTSN 4.;
LABEL NPLTOTSN="Total Characters Sent";
NPLTOTSN = SUM(NPLNRFMS,NPLNRNFS);
;
/* Data Element Derivation (NPLTOTRC) */;
FORMAT NPLTOTRC 4.;
LABEL NPLTOTRC="Total Characters Received";
NPLTOTRC = SUM(NPLNRFMR,NPLNRNFR);
```

```

;
/* Data Element Derivation (NPLTOTTR) */;
FORMAT NPLTOTTR 4.;
LABEL NPLTOTTR="Total Characters Transmitted";
NPLTOTTR = SUM(NPLNRFMR,NPLNRNFR,NPLNRFMS,NPLNRNFS);
;
/* Data Element Derivation (NPLAVCHS) */;
FORMAT NPLAVCHS 4.;
LABEL NPLAVCHS="AVERAGE CHARACTERS SENT";
NPLAVCHS = .;
NPLNRFMR=SUM(NPLNRFMS,NPLNRNFS);
IF NPLTRES GT 0 THEN NPLAVCHS=NPLNRFMR/NPLTRES;
;
/* Data Element Derivation (NPLAVCHR) */;
FORMAT NPLAVCHR 4.;
LABEL NPLAVCHR="AVERAGE CHARACTERS RECEIVED";
NPLAVCHR = .;
NPLNRFRE=SUM(NPLNRFMR,NPLNRNFR);
IF NPLTRES NE 0 THEN NPLAVCHR=NPLNRFRE/NPLTRES;
;
/* Data Element Derivation (NPLAVCHT) */;
FORMAT NPLAVCHT 4.;
LABEL NPLAVCHT="AVERAGE TOTAL CHARACTERS TRANSMITTED";
NPLAVCHT = .;
NPLTOCTR=SUM(NPLNRFMR,NPLNRNFR,NPLNRFMS,NPLNRNFS);
IF NPLTRES NE 0 THEN NPLAVCHT=NPLTOCTR/NPLTRES;
;
/* Data Element Derivation (NPLAVPIU) */;
FORMAT NPLAVPIU SCALE4.;
LABEL NPLAVPIU="AVERAGE PIUS PER/RESPONSE";
NPLAVPIU = .;
NPLNRPIU=SUM(NPLNRPFMS,NPLNRPFMR);
IF NPLTRES GT 0 THEN NPLAVPIU=NPLNRPIU/NPLTRES;
;

```

USAGE CONSIDERATIONS:

All cycles are summarized together as a data range rather than reporting by individual cycle or by year, month, day, and hour as other CA MICS reports do.

1

(SNTLDQ) DAILY NPM APPLICATION/LINK RANKING BY ZONE
FIRST 10 APPLICATIONS BY DESCENDING AVERAGE TOTAL RESPONSE TIME
NETWORK ID: NETWORK1 SYSTEM ID: SYS1 DATA RANGE: 040CTyy-040CTyy ZONE: 1

-IDENTIFICATION--		RESPONSE INFORMATION										WORKLOAD INFORMATION					
LINK NAME /		AVG TIME			NOT IN	TOTAL			RATE	% WITH	TOTAL CHARS			AVG CHARS			PIUS /
APPLICATION NAME		TOTAL	HOST	NET	RANGE	RANGE	RESPS	/ MIN	NET TM	SENT	RECD	TRANS	SENT	RECD	TRANS	RESP	
L12131	DISOSS20	5.70	5.70	0.00	83	0.0-5.0	153	3.48	0.00%	7K	13K	20K	48	88	137	2.02	
L2A001	TS00046	4.87	0.94	3.92	2	0.0-5.0	10	0.23	100.0%	7K	211	7K	710	21	732	3.80	
L12031	CHRSDC2	4.86	2.98	1.89	14	0.0-5.0	224	3.82	99.55%	361K	15K	377K	1K	70	1K	2.04	
L12046	CHRSDC2	3.78	2.35	1.44	22	0.0-5.0	123	2.49	100.0%	139K	9K	149K	1K	77	1K	2.72	
L12023	CHRSDC2	3.66	1.87	1.78	29	0.0-5.0	145	2.16	100.0%	198K	8K	206K	1K	59	1K	2.65	
L12141	DISOSS20	3.55	3.55	0.00	16	0.0-5.0	36	2.11	0.00%	35K	3K	39K	987	107	1K	2.86	
L2A178	TS00025	3.27	1.57	1.69	9	0.0-5.0	67	0.89	100.0%	57K	1K	59K	862	24	887	2.21	
L2A178	TS00020	3.22	1.65	1.57	10	0.0-5.0	78	1.40	100.0%	87K	1K	89K	1K	20	1K	2.19	
L12027	ISSA1	3.09	3.09	0.00	2	0.0-5.0	5	4.05	0.00%	3K	102	3K	679	20	699	5.00	
L2A178	TS00024	2.74	1.07	1.67	6	0.0-5.0	51	0.93	100.0%	46K	927	47K	914	18	932	2.16	

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NPLAVTTM=AVERAGE TOTAL RESPONSE TIME
RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NPL

Figure 3-

3.3.1.1.13 NetSpy Application Service/Workload Ranking

INTENDED USE:

To rank all or selected applications in ascending or descending order based on response times or character traffic volumes. The user chooses the number of applications ranked, the order of ranking, and the variable used to rank on. The report provides both response and workload information that can be used to identify applications having high traffic volumes or response times.

FORMAT:

A 18 column report approximately 132 characters wide. It is best suited for hardcopy review but can be reviewed online. The information is summarized and presented by NETWKID, SYSID, PLU, Data Range, and Zone or Zone by Hour.

INQUIRY ID:

SNTLD2 - Application w/in zone
SNTLD3 - Application w/in hour

DATA SOURCE (File/Timespan):

SNTNSP - Days

DATA ELEMENTS USED:

DURATION, PLU, NSPAVTTM, NSPAVHTM, NSPAVNTM, NSPRDST5, IQ, RANGE, NSPTRESC, NSPTRSMN, NSPPCNTM, NSPNRBYS, NSPNRBYSR, NSPTOTTR, NSPAVCHS, NSPAVCHR, NSPAVCHT, RDSTTYPE, SYSID, PLUMSMGR, NETWKID, DATA, ZONE, RANKELEM, RANKLBL, DATE, CURRENT, TIME

CALCULATIONS:

```
/* Data Element Derivation (DATE) */;
FORMAT DATE DATE7.;
LABEL DATE="Date Selection Field";
DATE = DATEPART(ENDTS);
;
/* Data Element Derivation (TIME) */;
FORMAT TIME TIME11.2;
LABEL TIME="Time Selection Field";
TIME = TIMEPART(ENDTS);
```

```
;
/* Data Element Derivation (DATA) */;
LENGTH DATA $15;
FORMAT DATA $CHAR15.;
LABEL DATA="DATA RANGE";
DATA = ' ';
/* SAS System Statements(Derive vars & data select) */;
RETAIN DATEA DATEB;
LENGTH DATEA DATEB 4.;
DATEA = MIN(DATEA,STARTTS);
DATEB = MAX(DATEB,ENDTS);
IF _EOF_ THEN DO;
    DATEA=DATEPART(DATEA);
    DATEB=DATEPART(DATEB);
    SUBSTR(DATA,1,7)=PUT(DATEA,DATE7.);
    SUBSTR(DATA,8,1)='- ';
    SUBSTR(DATA,9,7)=PUT(DATEB,DATE7.);
    CALL SYMPUT('S',DATA);
    %GLOBAL S;
    DROP DATEA DATEB;
END;
/* Data Summarization */
%MACRO NEGATE;
    DATA=SYMGET('S');
%MEND NEGATE;
;
/* Data Element Derivation (RANGE) */;
LENGTH RANGE $7;
FORMAT RANGE $CHAR7.;
LABEL RANGE="LOW-HI TOTAL RESPONSE THRESHOLD";
RANGE = ' ';
SUBSTR(RANGE,1,3)=PUT(NSPRVAL1,3.1);
SUBSTR(RANGE,4,1)='- ';
SUBSTR(RANGE,5,3)=PUT(NSPRVAL4,3.1);
;
/* Data Element Derivation (CURRENT, &C) */;
FORMAT CURRENT WEEKDATE15.;
LABEL CURRENT="CURRENT DATE";
CURRENT = TODAY();
C=PUT(CURRENT,WEEKDATE15.);
C=COMPRESS(C) ;
CALL SYMPUT('C',PUT(C,$CHAR12.));
%GLOBAL C;
;
/* Data Element Derivation (IQ, &I) */;
LENGTH IQ $8;
FORMAT IQ $CHAR8.;
LABEL IQ="Inquire Name";
IQ = ' ';
```

```

SUBSTR(IQ,1,1)='(';
SUBSTR(IQ,2,6)=SYMGET('INQINAME');
SUBSTR(IQ,8,1)=')';
CALL SYMPUT('I',PUT(IQ,$CHAR8.));
%GLOBAL I;
;
/* Data Element Derivation (RANKELEM) */;
FORMAT RANKELEM 8.;
LABEL RANKELEM="&RL";
RANKELEM = &RANKELEM;
;
/* Data Element Derivation (RANKLBL) */;
LENGTH RANKLBL $40;
FORMAT RANKLBL $CHAR40.;
LABEL RANKLBL="LABEL OF RANKING ELEMENT";
RANKLBL = SYMGET('RL');
;
/* Data Element Derivation (NSPPCNTM) */;
LENGTH NSPPCNTM $6;
FORMAT NSPPCNTM $CHAR6.;
LABEL NSPPCNTM="% RESPONSES WITH NETWORK TIME";
NSPPCNTM = '    %';
IF NSPTRESC GT 0 THEN
    NSPPCNON=((NSPTRESC-NSPNRESC)/NSPTRESC);
ELSE NSPPCNON=100;
IF NSPPCNON GT 0 THEN NSPTNETM=(100.0-NSPPCNON);
SUBSTR(NSPPCNTM,1,5)=PUT(NSPTNETM,5.2);
IF NSPTNETM EQ . THEN SUBSTR(NSPPCNTM,6,1)=' '; ;
;
/* Data Element Derivation (NSPTRSMN) */;
FORMAT NSPTRSMN SCALE4.;
LABEL NSPTRSMN="TRANSACTIONS PER MINUTE";
NSPTRSMN = .;
DURMINS=(DURATION/60);
IF DURMINS GT 0 THEN NSPTRSMN=NSPTRESC/DURMINS;
;
/* Data Element Derivation (NSPTOTTR) */;
FORMAT NSPTOTTR SCALE4.;
LABEL NSPTOTTR="TOTAL CHARACTERS TRANSMITTED";
NSPTOTTR = SUM(NSPNRBYR,NSPNRBYS);
;
/* Data Element Derivation (NSPAVCHS) */;
FORMAT NSPAVCHS SCALE4.;
LABEL NSPAVCHS="AVERAGE CHARACTERS SENT";
NSPAVCHS = .;
IF NSPTRESC GT 0 THEN NSPAVCHS=NSPNRBYS/NSPTRESC;
;
/* Data Element Derivation (NSPAVCHR) */;
FORMAT NSPAVCHR SCALE4.;

```

```

LABEL NSPAVCHR="AVERAGE CHARACTERS RECEIVED";
NSPAVCHR = .;
IF NSPTRESC NE 0 THEN NSPAVCHR=NSPNRBYR/NSPTRESC;
;
/* Data Element Derivation (NSPAVCHT) */;
FORMAT NSPAVCHT SCALE4.;
LABEL NSPAVCHT="AVERAGE TOTAL CHARACTERS TRANSMITTED";
NSPAVCHT = .;
NSPTOCTR=SUM(NSPNRBYR,NSPNRBY);
IF NSPTRESC NE 0 THEN NSPAVCHT=NSPTOCTR/NSPTRESC;
;

```

USAGE CONSIDERATIONS:

All cycles are summarized together as a data range rather than reporting by individual cycle or by year, month, day, and hour as other CA MICS reports do.

1

(SNTLD2) DAILY NETSPY APPLICATION RANKING BY ZONE																	
FIRST 10 APPLICATIONS BY DESCENDING AVERAGE TOTAL RESPONSE TIME																	
NETWORK ID: NETWORK1		SYSTEM ID: SYS1		DATA RANGE: 05DECyy-29JULyy						ZONE: 1							
-IDENTIFICATION--		RESPONSE INFORMATION										WORKLOAD INFORMATION					
DURATION(HH:MM) /		---- AVG TIME ----		NOT IN		TOTAL		RATE		% WITH		--- TOTAL CHARS ---		----- AVG CHARS -----		RESP SES	
APPLICATION NAME		TOTAL	HOST	NET	RANGE	RANGE	RESPS	/ MIN	NET TM	SENT	RECVD	TRANS	SENT	RECVD	TRANS	TYPE	MGR
=====		=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====	=====
9:00	A55ITPXX	2.15	2.11	0.04	6	1.0- 10	1K	1	.	1M	14K	1M	1K	13	1K	USER	N
9:00	A31ITS0	1.83	1.83	0.00	0	0.0-0.0	907	1	99.00%	1M	19K	1M	1K	21	1K	USER	N
9:00	A11ITS0	0.33	0.27	0.07	150K	0.0-0.0	162K	300	99.93%	196M	144M	340M	1K	890	2K	USER	N
9:00	STNM4	0.27	0.24	0.03	0	1.0- 10	240	0	.	394K	3K	397K	1K	15	1K	USER	N
9:00	A03ACC1H	0.00	0.00	0.00	0	1.0- 10	0	0	0.00%	0	0	0	0	0	0	USER	N
9:00	A44DEN44	0.00	0.00	0.00	0	2.0- 30	0	0	0.00%	0	0	0	0	0	0	USER	N
9:00	A44ITS0	0.00	0.00	0.00	0	0.0-0.0	0	0	0.00%	0	0	0	0	0	0	USER	N
9:00	A55IITPX	0.00	0.00	0.00	0	0.0-0.0	0	0	0.00%	0	0	0	0	0	0	USER	N
9:00	A71ITS0	0.00	0.00	0.00	0	0.0-0.0	0	0	0.00%	0	0	0	0	0	0	USER	N
9:00	CSNM21	0.00	0.00	0.00	0	1.0- 10	1	0	99.00%	2K	2K	4K	2K	2K	4K	USER	N

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NSPAVTM=AVERAGE TOTAL RESPONSE TIME
RUN-DATE=Wed,Sep3,yy , TIMESpan=DAYS, DBID=8, FILE=NSP

2

(SNTLD2) DAILY NETSPY APPLICATION RANKING BY ZONE																							
FIRST 10 APPLICATIONS BY DESCENDING AVERAGE TOTAL RESPONSE TIME																							
NETWORK ID: NETWORK1			SYSTEM ID: SYS2			DATA RANGE: 05DECyy-29JULyy			ZONE: 2														
-IDENTIFICATION- -			----- RESPONSE INFORMATION -----						----- WORKLOAD INFORMATION -----														
DURATION(HH:MM) /			--- AVG TIME ---			NOT IN			TOTAL RATE			--- TOTAL CHARS ---			--- AVG CHARS ---			RESP SES					
APPLICATION NAME			TOTAL HOST NET			RANGE			RANGE RESPS			/ MIN NET TM			SENT RECVD TRANS			SENT RECVD TRANS			TYPE MGR		
=====			=====			=====			=====			=====			=====			=====			=====		
20:30	A31ITS0		7.38	7.38	0.00	0	0.0-0.0		1K	1	99.00%	1M	25K	1M	909	14	923	USER	N				
20:30	DENM1811		0.99	0.71	0.29	2	1.0- 10		181	0	.	344K	1K	346K	1K	10	1K	USER	N				
20:30	QANM1211		0.93	0.64	0.29	8	1.0- 10		431	0	.	127M	5K	127M	295K	13	295K	USER	N				
20:30	QANM931		0.55	0.29	0.26	0	1.0- 10		11	0	99.91%	2M	5M	7M	231K	457K	689K	USER	N				
20:30	DENM1731		0.52	0.26	0.26	0	1.0- 10		60	0	.	45K	1K	46K	752	16	769	USER	N				
20:30	QANM9NS		0.48	0.00	0.48	0	1.0- 10		149	0	.	183K	479K	662K	1K	3K	4K	USER	N				
20:30	A11ITS0		0.40	0.27	0.12	60K	0.0-0.0		74K	60	99.81%	111M	10M	121M	1K	143	1K	USER	N				
20:30	STNM4		0.39	0.13	0.27	0	1.0- 10		1K	0	.	1M	28K	1M	1K	23	1K	USER	N				
20:30	A55ITPXX		0.11	0.10	0.02	0	1.0- 10		4	0	.	7K	61	8K	1K	15	2K	USER	N				
20:30	A03ACC1H		0.00	0.00	0.00	0	1.0- 10		0	0	0.00%	0	0	0	0	0	0	USER	N				
DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NSPAVTM=AVERAGE TOTAL RESPONSE TIME																							
RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NSP																							

```

(SNTLD2) DAILY NETSPY APPLICATION RANKING BY ZONE
FIRST 10 APPLICATIONS BY DESCENDING AVERAGE TOTAL RESPONSE TIME
NETWORK ID: NETWORK1 SYSTEM ID: SYS3 DATA RANGE: 05DECyy-29JULyy ZONE: 3
|-IDENTIFICATION--||----- RESPONSE INFORMATION -----||----- WORKLOAD INFORMATION -----|
|DURATION(HH:MM) /| |---- AVG TIME ----| NOT IN | TOTAL RATE % WITH| |--- TOTAL CHARS ---| |---- AVG CHARS ----| |RESP SES|
|APPLICATION NAME |||TOTAL HOST NET | |RANGE RANGE RESPS / MIN NET TM|||SENT RECVD TRANS| |SENT RECVD TRANS| |TYPE MGR|
|=====|
20:15 A11ITS0 0.32 0.22 0.10 8K 0.0-0.0 11K 9 99.78% 14M 225K 14M 1K 20 1K USER N
20:15 STNM4 0.15 0.06 0.09 0 1.0- 10 79 0 . 74K 1K 75K 944 17 961 USER N
20:15 A03ACC1H 0.00 0.00 0.00 0 1.0- 10 0 0 0.00% 0 0 0 0 0 0 0 USER N
20:15 A31ITS0 0.00 0.00 0.00 0 0.0-0.0 0 0 0.00% 0 0 0 0 0 0 0 USER N
20:15 A44DEN44 0.00 0.00 0.00 0 2.0- 30 0 0 0.00% 0 0 0 0 0 0 0 USER N
20:15 A44ITS0 0.00 0.00 0.00 0 0.0-0.0 0 0 0.00% 0 0 0 0 0 0 0 USER N
20:15 A55IITPX 0.00 0.00 0.00 0 0.0-0.0 0 0 0.00% 0 0 0 0 0 0 0 USER N
20:15 A55ITPXX 0.00 0.00 0.00 0 1.0- 10 0 0 0.00% 0 0 0 0 0 0 0 USER N
20:15 A71ITS0 0.00 0.00 0.00 0 0.0-0.0 0 0 0.00% 0 0 0 0 0 0 0 USER N
20:15 CSNM21 0.00 0.00 0.00 0 1.0- 10 0 0 0.00% 0 0 0 0 0 0 0 USER N
|=====|

```

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NSPAVTTM=AVERAGE TOTAL RESPONSE TIME
 RUN-DATE=Wed_Sep3.yy, TIMESpan=DAYS, DBID=8, FILE=NSP

(SNTLD2) DAILY NETSPY APPLICATION RANKING BY ZONE																			
FIRST 10 APPLICATIONS BY DESCENDING AVERAGE TOTAL RESPONSE TIME																			
NETWORK ID: NETWORK1			SYSTEM ID: SY55			DATA RANGE: 05DECyy-29JULyy			ZONE: 1										
RESPONSE INFORMATION										WORKLOAD INFORMATION									
-IDENTIFICATION--		DURATION(HH:MM) /		AVG TIME		NOT IN		TOTAL		RATE		% WITH		TOTAL CHARS		AVG CHARS		RESP SES	
APPLICATION NAME		TOTAL	HOST	NET	RANGE	RANGE	RESPS	/ MIN	NET TM	SENT	RECVD	TRANS	SENT	RECVD	TRANS	TYPE	MGR		
2:40	SCON28	4.24	2.23	2.01	82	1.0- 10	828	5	99.80%	34M	14K	34M	41K	18	41K	USER	N		
2:40	TS008	2.95	2.95	0.00	0	1.0- 10	3	0	99.00%	1K	60	1K	483	20	503	USER	N		
2:40	TS028	2.68	1.74	0.94	338	1.0- 10	6K	39	100.0%	4M	129K	5M	780	20	800	USER	N		
2:40	TPXPROD	2.29	2.29	0.00	0	- - -	1	0	99.00%	2K	95	2K	2K	95	2K	USER	Y		
2:40	VM10	1.33	1.33	0.00	0	1.0- 10	3	0	99.00%	3K	47	3K	1K	15	1K	USER	N		
2:40	NSTONY	1.08	0.47	0.61	6	1.0- 10	295	1	.	608K	6K	615K	2K	22	2K	USER	N		
2:40	LMNOPQ08	0.00	0.00	0.00	0	0.0-0.0	0	0	0.00%	0	0	0	0	0	0	USER	N		
2:40	NCCF1	0.00	0.00	0.00	0	1.0- 10	0	0	0.00%	0	0	0	0	0	0	USER	N		
2:40	NETSPYES	0.00	0.00	0.00	0	1.0-2.0	0	0	0.00%	0	0	0	0	0	0	USER	N		
2:40	NETSPYSP	0.00	0.00	0.00	0	1.0- 10	0	0	0.00%	0	0	0	0	0	0	USER	N		

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NSPAVTTM=AVERAGE TOTAL RESPONSE TIME

RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NSP

6

(SNTLD2) DAILY NETSPY APPLICATION RANKING BY ZONE																						
FIRST 10 APPLICATIONS BY DESCENDING AVERAGE TOTAL RESPONSE TIME																						
NETWORK ID: NETWORK1			SYSTEM ID: SYS6			DATA RANGE: 05DECyy-29JULyy			ZONE: 2													
-IDENTIFICATION- -			----- RESPONSE INFORMATION -----			----- WORKLOAD INFORMATION -----																
DURATION(HH:MM) /			--- AVG TIME ---			NOT IN			TOTAL RATE			--- TOTAL CHARS ---			--- AVG CHARS ---			RESP SES				
APPLICATION NAME			TOTAL HOST NET			RANGE			RESPS / MIN			NET TM			SENT RECVD TRANS			SENT RECVD TRANS			TYPE MGR	
=====			=====			=====			=====			=====			=====			=====				
0:44	NSTONY	1.01	0.01	1.01	0	1.0- 10	77	1	.	297K	1K	298K	3K	13	3K	USER	N					
0:44	TS028	0.31	0.27	0.04	5	1.0- 10	1K	24	.	777K	15K	793K	708	14	723	USER	N					
0:44	SCON28	0.03	0.02	0.02	0	1.0- 10	264	6	99.87%	2M	4K	2M	10K	17	10K	USER	N					
0:44	LMNOPQ08	0.00	0.00	0.00	0	0.0-0.0	0	0	0.00%	0	0	0	0	0	0	USER	N					
0:44	NCCF1	0.00	0.00	0.00	0	1.0- 10	0	0	0.00%	0	0	0	0	0	0	USER	N					
0:44	NETSPYES	0.00	0.00	0.00	0	1.0-2.0	0	0	0.00%	0	0	0	0	0	0	USER	N					
0:44	NETSPYSP	0.00	0.00	0.00	0	1.0- 10	0	0	0.00%	0	0	0	0	0	0	USER	N					
0:44	NETSPYVM	0.00	0.00	0.00	0	1.0- 10	0	0	0.00%	0	0	0	0	0	0	USER	N					
0:44	NETSPYXA	0.00	0.00	0.00	0	1.0-2.0	0	0	0.00%	0	0	0	0	0	0	USER	N					
0:44	NETSPY06	0.00	0.00	0.00	0	1.0-2.0	0	0	0.00%	0	0	0	0	0	0	USER	N					
DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NSPAVTTM=AVERAGE TOTAL RESPONSE TIME																						
RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NSP																						

(SNTLD2) DAILY NETSPY APPLICATION RANKING BY ZONE																	
FIRST 10 APPLICATIONS BY DESCENDING AVERAGE TOTAL RESPONSE TIME																	
NETWORK ID: NETWORK1			SYSTEM ID: SYS7			DATA RANGE: 05DECyy-29JULyy			ZONE: 1								
RESPONSE INFORMATION										WORKLOAD INFORMATION							
IDENTIFICATION--		-----		-----		-----		-----		-----		-----		-----		-----	
DURATION(HH:MM) /		----		AVG TIME ----		NOT IN		TOTAL RATE		% WITH		--- TOTAL CHARS ---		----- AVG CHARS ----		RESP SES	
APPLICATION NAME		TOTAL		HOST		NET		RANGE		RANGE		RESPS		/ MIN		NET TM	
SENT		RECVD		TRANS		SENT		RECVD		TRANS		TYPE		MGR			
2:40 NSTONY		9.44	6.22	3.22	14	1.0- 10	77	0	.	151K	1K	153K	1K	23	1K	USER	N
2:40 LMNOPQ08		0.00	0.00	0.00	0	0.0-0.0	0	0	0.00%	0	0	0	0	0	0	USER	N
2:40 NCCF1		0.00	0.00	0.00	0	1.0- 10	0	0	0.00%	0	0	0	0	0	0	USER	N
2:40 NETSPYES		0.00	0.00	0.00	0	1.0-2.0	0	0	0.00%	0	0	0	0	0	0	USER	N
2:40 NETSPYSP		0.00	0.00	0.00	0	1.0- 10	0	0	0.00%	0	0	0	0	0	0	USER	N
2:40 NETSPYVM		0.00	0.00	0.00	0	1.0- 10	0	0	0.00%	0	0	0	0	0	0	USER	N
2:40 NETSPYXA		0.00	0.00	0.00	0	1.0-2.0	0	0	0.00%	0	0	0	0	0	0	USER	N
2:40 NETSPY06		0.00	0.00	0.00	0	1.0-2.0	0	0	0.00%	0	0	0	0	0	0	USER	N
2:40 NSTEST		0.00	0.00	0.00	0	1.0- 10	0	0	0.00%	0	0	0	0	0	0	USER	N
2:40 RMT1		0.00	0.00	0.00	0	0.0-0.0	0	0	0.00%	0	0	0	0	0	0	USER	N

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NSPAVTTM=AVERAGE TOTAL RESPONSE TIME
RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NSP

(SNTLD2) DAILY NETSPY APPLICATION RANKING BY ZONE																			
FIRST 10 APPLICATIONS BY DESCENDING AVERAGE TOTAL RESPONSE TIME																			
NETWORK ID: NETWORK1			SYSTEM ID: SYS8			DATA RANGE: 05DECyy-29JULyy			ZONE: 1										
-IDENTIFICATION- -			----- RESPONSE INFORMATION -----									----- WORKLOAD INFORMATION -----							
DURATION(HH:MM) /			--- AVG TIME ---			NOT IN			TOTAL RATE			--- TOTAL CHARS ---			--- AVG CHARS ---			RESP SES	
APPLICATION NAME			TOTAL HOST NET			RANGE			RESPS / MIN			SENT RECVD TRANS			SENT RECVD TRANS			TYPE MGR	
0:15	A44SJES2		3.72	3.72	0.00	0	0.0-0.0		56	3	99.00%	7M	20K	7M	128K	361	129K	USER	N
0:15	A44ISP30		0.47	0.42	0.05	1	2.0- 30		75	5	.	64K	1K	65K	858	16	875	USER	N
0:15	A44ITPXI		0.44	0.27	0.17	0	. - .		236	15	99.97%	238K	5K	243K	1K	22	1K	USER	Y
0:15	A44ITS0		0.37	0.20	0.17	4	2.0- 30		3K	204	100.0%	3M	59K	3M	1K	19	1K	USER	N
0:15	A01ITS0		0.23	0.05	0.18	0	2.0- 30		157	10	99.88%	127K	1K	129K	815	9	824	USER	N
0:15	A04IACCW		0.00	0.00	0.00	0	2.0- 30		0	0	0.00%	0	0	0	0	0	0	USER	N
0:15	A04IACCX		0.00	0.00	0.00	0	2.0- 30		0	0	0.00%	0	0	0	0	0	0	USER	N
0:15	A04IACCY		0.00	0.00	0.00	0	2.0- 30		0	0	0.00%	0	0	0	0	0	0	USER	N
0:15	A04IACCZ		0.00	0.00	0.00	0	2.0- 30		0	0	0.00%	0	0	0	0	0	0	USER	N
0:15	A04ICCS1		0.00	0.00	0.00	0	2.0- 30		0	0	0.00%	0	0	0	0	0	0	USER	N
DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NSPAVTTM=AVERAGE TOTAL RESPONSE TIME																			
RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NSP																			

(SNTLD2) DAILY NETSPY APPLICATION RANKING BY ZONE																			
FIRST 10 APPLICATIONS BY DESCENDING AVERAGE TOTAL RESPONSE TIME																			
NETWORK ID: NETWORK1				SYSTEM ID: SYS9			DATA RANGE: 05DECyy-29JULyy				ZONE: 2								
-IDENTIFICATION--		RESPONSE INFORMATION										WORKLOAD INFORMATION							
DURATION(HH:MM) /		AVG TIME ----			NOT IN		TOTAL		RATE		% WITH		TOTAL CHARS ---			AVG CHARS ----		RESP SES	
APPLICATION NAME		TOTAL	HOST	NET	RANGE	RANGE	RESPS	/ MIN	NET TM	SENT	RECD	TRANS	SENT	RECD	TRANS	TYPE	MGR		
0:30	A44ISP40	1.20	1.15	0.05	5	2.0- 30	627	20	100.0%	899K	607K	1M	1K	968	2K	USER	N		
0:30	A44ITS0	0.32	0.21	0.12	1	2.0- 30	1K	52	99.97%	2M	21K	2M	1K	13	1K	USER	N		
0:30	A44ISYVW	0.12	0.10	0.03	0	2.0- 30	11	0	99.45%	24K	349	25K	2K	31	2K	USER	N		
0:30	A44SJES2	0.09	0.09	0.00	0	0.0-0.0	6	0	99.00%	18K	585K	604K	3K	97K	100K	USER	N		
0:30	A44ITPXJ	0.06	0.02	0.04	0	. - .	670	22	100.0%	925K	6K	932K	1K	9	1K	USER	Y		
0:30	A01ITS0	0.00	0.00	0.00	0	2.0- 30	0	0	0.00%	0	0	0	0	0	0	USER	N		
0:30	A04ICCS1	0.00	0.00	0.00	0	2.0- 30	0	0	0.00%	0	0	0	0	0	0	USER	N		
0:30	A04ICI33	0.00	0.00	0.00	0	2.0- 30	0	0	0.00%	0	0	0	0	0	0	USER	N		
0:30	A04ICL	0.00	0.00	0.00	0	2.0- 30	0	0	0.00%	0	0	0	0	0	0	USER	N		
0:30	A04ICLUK	0.00	0.00	0.00	0	2.0- 30	0	0	0.00%	0	0	0	0	0	0	USER	N		

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NSPAVTTM=AVERAGE TOTAL RESPONSE TIME
RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NSP

Figure 3-

3.3.1.1.14 TSO Resp Time Components

INTENDED USE:

Use this chart to determine, for TSO, what portion of average total response time occurs in the host versus that which occurs in the network.

FORMAT:

This display produces a stacked vertical bar chart showing the components of average total response time (host and network) by hour for TSO.

INQUIRY ID:

Color Graphics: SNTCDO

Printer Graphics: N/A

DATA SOURCE (File/Timespan):

SNTNSP, TSOTSU - Previous day

DATA ELEMENTS USED:

HOUR, PLU, NSPAVNTM, TSUCPUTM, TSUTRESC, TSUTRSTM,
TSUSIDTM, TSUSINTM

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This report combines user activity data that CA TSO/MON PM collects and stores in the TSOTSU file with application activity data that CA NetSpy collects and stores in the SNTNSP file. To merge these two files, resummaries the TSOTSU file so it has the same sequence summary keys as the SNTNSP file. For this inquiry to do this resummation, it must create the NETWRKID element in the TSOTSU file and populate it using the PARMS member contained in prefix.MICS.PARMS(SNTNIDRT).

WARNING! For the reasons described above, in the MICF execution time options for this inquiry, you must specify the ddname for allocating prefix.MICS.PARMS. Otherwise, this inquiry will abend. For further information on how to tailor the inquiry to allocate prefix.MICS.PARMS, see MICF Options in the MICF Reference Guide.

3.3.1.2 Reliability Analysis Inquiries

Reliability analysis inquiries provide statistics regarding temporary or permanent errors caused by network components, and also indicate the number and type of abnormal UNBINDs (disruptions to a terminal user's session with a host application). Each inquiry is discussed in greater detail in the following sections:

- 1 - NPM Daily Link Error Count
- 2 - NPM/NetSpy Daily Link Error Count
- 3 - NetView Daily % Link Errors to Traffic
- 4 - NetView Daily NPDA Events Summary
- 5 - NetView Weekly Abnormal UNBINDs by PLU
- 6 - NetView Weekly Abnormal UNBIND Report
- 7 - NetView Events Ranking
- 8 - NetView Events by Resource Type Ranking
- 9 - NetView Events by Resource Ranking
- 10 - NPDA Daily Resource Alert Summary
- 11 - NPDA Daily Resource Alert Description
- 12 - NPDA Detail Generic Alert Report
- 13 - NPDA Daily Alerts by Resource Type
- 14 - NPDA Daily Alerts by Problem Type

3.3.1.2.1 NPM Daily Link Error Count

INTENDED USE:

This chart is used to show the count of temporary errors that the network control program detects in network line components during the measurement interval.

FORMAT:

This display produces a vertical bar chart of error counts by hour for an individual link.

INQUIRY ID:

Color Graphics: SNTCD9

Printer Graphics: N/A

DATA SOURCE (File/Timespan):

SNTNCL01 - Previous day

DATA ELEMENTS USED:

HOURL, NETNAME, NCLNRERR

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This inquiry is produced from NetView Performance Monitor (NPM) network data.

3.3.1.2.2 NPM/NetSpy Daily Link Error Count

INTENDED USE:

This chart is used to show the count of temporary errors that the network control program detects in network line components during the measurement interval.

FORMAT:

This display produces a vertical bar chart of error counts by hour for an individual link.

INQUIRY ID:

Color Graphics: N/A
Printer Graphics: SNTPD9

DATA SOURCE (File/Timespan):

SNTNCL01 - Previous day

DATA ELEMENTS USED:

HOURL, NETNAME, NCLNRERR

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This inquiry is produced from NetView Performance Monitor (NPM) network data or CA NetSpy N-Record data.

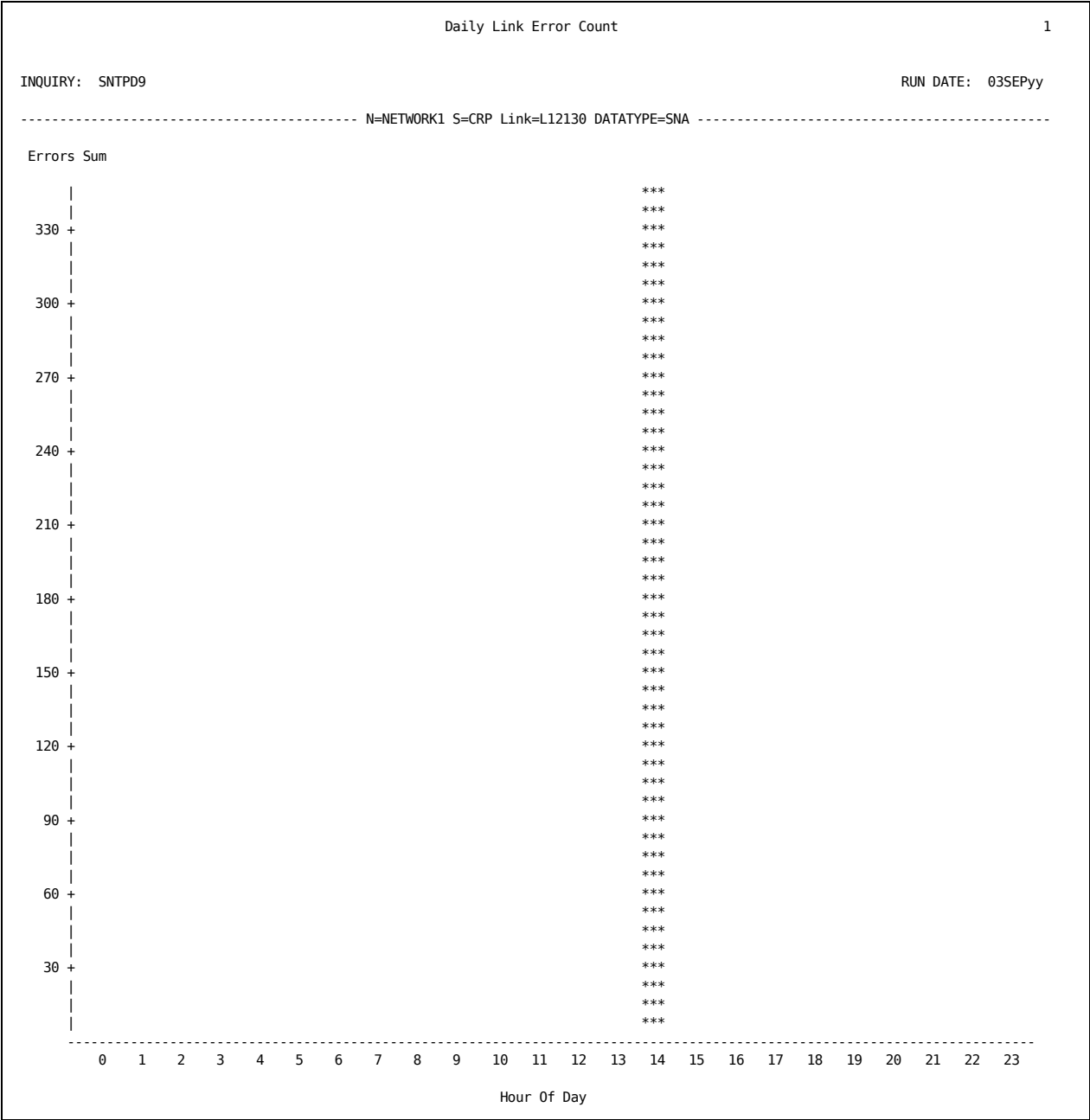


Figure 3-

3.3.1.2.3 NetView Daily % Link Errors to Traffic

INTENDED USE:

This chart is used to show increases in the percentage of temporary errors to total line traffic over a period of 24 hours.

FORMAT:

This display produces a vertical bar chart showing the percentage of temporary errors to total line traffic as reported by NetView Hardware Monitor/NPDA.

INQUIRY ID:

Color Graphics: SNTCDA
Printer Graphics: SNTPDA

DATA SOURCE (File/Timespan):

SNTNSF01 - Previous day

DATA ELEMENTS USED:

HOURL, NSFFRNAM, NSFPCERR

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This inquiry is produced from NetView Hardware Monitor/NPDA data. An increase in the ratio of temporary errors to character traffic on the line may indicate a network component that failed somewhere along the line. This should be investigated.

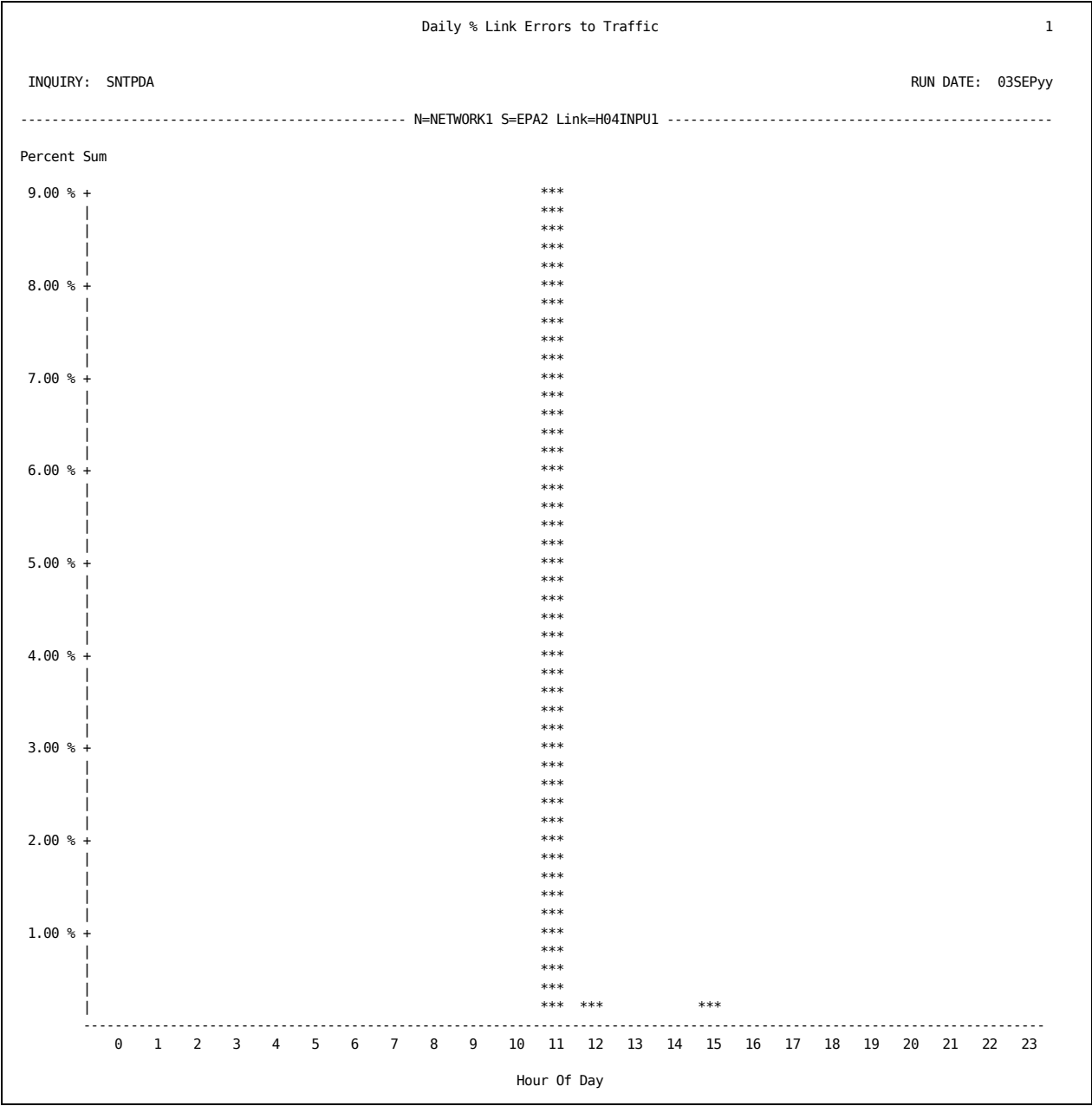


Figure 3-

3.3.1.2.4 NetView Daily NPDA Events Summary

INTENDED USE:

This chart is used to show events that are recorded because the percent of temporary errors to line traffic threshold has been exceeded, or because some other user-defined event has occurred. A high or increasing number of events over a period of 24 hours indicates the need for a detailed investigation of NetView Hardware Monitor/NPDA data for the cluster controller identified in this inquiry.

FORMAT:

This display produces a vertical bar chart of the number of site-defined events by cluster controller for each hour in the day.

INQUIRY ID:

Color Graphics: SNTCDB
Printer Graphics: SNTPDB

DATA SOURCE (File/Timespan):

SNTNEF01 - Previous day

DATA ELEMENTS USED:

HOURL, NEFFRNAM, NEFNREVT

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This inquiry is produced from NetView Hardware Monitor/NPDA data. You can investigate the NPDA Event Analysis report (SNT601), described in Section 3.1.3.6.1, to obtain the cause of each DETAIL event.

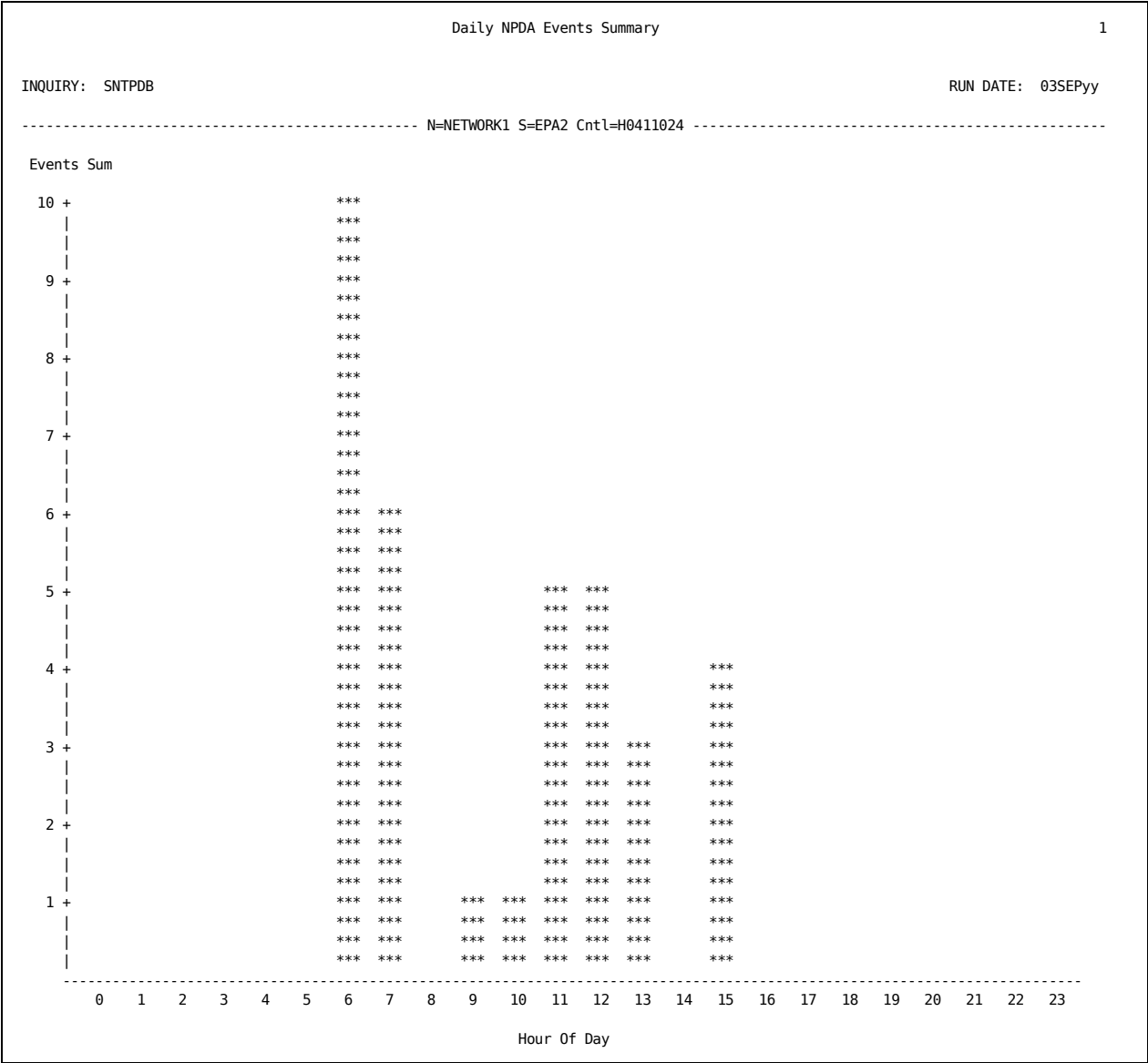


Figure 3-

3.3.1.2.5 NetView Weekly Abnormal UNBINDs by PLU

INTENDED USE:

This chart is used to record the number of abnormal UNBINDs that occur in each PLU during a week.

FORMAT:

This display produces a pie chart of the number of abnormal UNBINDs by primary logical unit (PLU) for the week.

INQUIRY ID:

Color Graphics: SNTCWJ

Printer Graphics: N/A

DATA SOURCE (File/Timespan):

NVSVBF01 - Previous day

DATA ELEMENTS USED:

VBFNRBF, PLU

CALCULATIONS:

None

USAGE CONSIDERATIONS:

An abnormal UNBIND is a disruptive termination of a terminal user's session with the host application. A large number of UNBINDs for an application indicates problems with either the application itself or with the network components used to access the application. An abnormal UNBIND is an UNBIND that occurs any other time than at 1) normal session end, or 2) when one application is passing a terminal session to another application.

3.3.1.2.6 NetView Weekly Abnormal UNBIND Report

INTENDED USE:

This report is used to identify, by primary logical unit (PLU), the 20 secondary logical units (SLUs) that have the highest number of UNBINDs for the week.

FORMAT:

This display produces a rank report of the 20 secondary logical units that have the highest number of abnormal UNBINDs for the week. These SLUs are listed (by PLU) in descending order of UNBIND frequency, along with UNBIND codes, the reasons for UNBIND, and the PLU that each terminal was in session with during UNBIND.

INQUIRY ID:

Color Graphics: N/A
Printer Graphics: SNTLW0

DATA SOURCE (File/Timespan):

NVSVBF01 - Previous day

DATA ELEMENTS USED:

VBFNRRBF, VBFCODE, VBFAUSE, SLU, PLU

CALCULATIONS:

None

USAGE CONSIDERATIONS:

An abnormal UNBIND is a disruptive termination of a terminal user's session with the host application. A large number of UNBINDs for an application indicates problems with either the application itself or with the network components used to access the application. An abnormal UNBIND is an UNBIND that occurs any other time than at 1) normal session end, or 2) when one application is passing a terminal session to another application.

20 SLUs With Most Abnormal UNBINDs For Week

1

INQUIRY: SNTLW0

RUN DATE: 03SEPyy

----- N=NETWORK1 S=SCNN -----

Number of Abnormal UNBINDS	UNBIND Code	UNBIND Reason	SLU	PLU
1	40	UNKNOWN VALUE	HOST59	

----- N=NETWORK1 S=SYSB -----

Number of Abnormal UNBINDS	UNBIND Code	UNBIND Reason	SLU	PLU
24	40	UNKNOWN VALUE	C42XM	
8	40	UNKNOWN VALUE	CL039003	C42XM
8	40	UNKNOWN VALUE	WKMGR002	C42XM
6	40	UNKNOWN VALUE	TL004001	C42XM
6	40	UNKNOWN VALUE	WIZ0002	C42XM
6	40	UNKNOWN VALUE	C41TS189	C42XM
5	40	UNKNOWN VALUE	C41TS055	C42XM
5	40	UNKNOWN VALUE	C41TS215	C42XM
5	40	UNKNOWN VALUE	C41TS241	C42XM
5	40	UNKNOWN VALUE	C41TS256	C42XM
5	40	UNKNOWN VALUE	C41TS195	C42XM
5	40	UNKNOWN VALUE	TL004003	C42XM
5	40	UNKNOWN VALUE	TL004002	C42XM
5	40	UNKNOWN VALUE	CL981126	C42XM
4	40	UNKNOWN VALUE	CFCTSWL	C42XM
4	40	UNKNOWN VALUE	CFCISA2	C42XM
4	40	UNKNOWN VALUE	CFCISBB	C42XM
4	40	UNKNOWN VALUE	C41TS245	C42XM
4	40	UNKNOWN VALUE	C41TS259	C42XM
4	40	UNKNOWN VALUE	C41TS025	C42XM

Figure 3-

3.3.1.2.7 NetView Events Ranking

INTENDED USE:

To rank all events in ascending or descending order based on frequency. The user chooses the order of ranking. The report provides both general and specific cause codes for each event listed. It is useful in identifying systems having high event activity.

FORMAT:

A 5 column report approximately 132 characters wide. It is best suited for hardcopy review but can be reviewed online. The information is summarized and presented by NETWRKID, SYSID, NEFEVGEN, NEFEVSPC, Data Range, and Zone or Zone by Hour.

INQUIRY ID:

SNTLDG - Events w/in zone
SNTLDH - Events w/in hour

DATA SOURCE (File/Timespan):

SNTNEF - Days

DATA ELEMENTS USED:

DURATION, NEFEVGEN, NEFEVSPC, NEFNREVT, NEFNRLT, RANKLBL, NETWRKID, SYSID, DATA, ZONE, DATE, TIME, IQ, CURRENT, RANKELEM

CALCULATIONS:

```
/* Data Element Derivation (DATE) */;
FORMAT DATE DATE7.;
LABEL DATE="Date Selection Field";
DATE = DATEPART(ENDTS);
;
/* Data Element Derivation (TIME) */;
FORMAT TIME TIME11.2;
LABEL TIME="Time Selection Field";
TIME = TIMEPART(ENDTS);
;
/* Data Element Derivation (DATA) */;
LENGTH DATA $15;
FORMAT DATA $CHAR15.;
LABEL DATA="DATA RANGE";
```

```
DATA = ' ';
/* SAS System Statements(Derive vars & data select) */;
RETAIN DATEA DATEB;
LENGTH DATEA DATEB 4.;
DATEA = MIN(DATEA,STARTTS);
DATEB=MAX(DATEB,ENDTS);
IF _EOF_ THEN DO;
    DATEA=DATEPART(DATEA);
    DATEB=DATEPART(DATEB);
    SUBSTR(DATA,1,7)=PUT(DATEA,DATE7.);
    SUBSTR(DATA,8,1)='- ';
    SUBSTR(DATA,9,7)=PUT(DATEB,DATE7.);
    CALL SYMPUT('S',DATA);
    %GLOBAL S;
    DROP DATEA DATEB;
END;
/* Data Summarization */
%MACRO NEGATE;
    DATA=SYMGET('S');
%MEND NEGATE;
;
/* Data Element Derivation (CURRENT, &C) */;
FORMAT CURRENT WEEKDATE15.;
LABEL CURRENT="CURRENT DATE";
CURRENT = TODAY();
C=PUT(CURRENT,WEEKDATE15.);
C=COMPRESS(C) ;
CALL SYMPUT('C',PUT(C,$CHAR12.));
%GLOBAL C;
;
/* Data Element Derivation (IQ, &I) */;
LENGTH IQ $8;
FORMAT IQ $CHAR8.;
LABEL IQ="Inquire Name";
IQ = ' ';
SUBSTR(IQ,1,1)='(';
SUBSTR(IQ,2,6)=SYMGET('INQINAME');
SUBSTR(IQ,8,1)=')';
CALL SYMPUT('I',PUT(IQ,$CHAR8.));
%GLOBAL I;
;
/* Data Element Derivation (DURATION, elapsed time) */;
FORMAT DURATION TIME5.2;
LABEL DURATION="ENDTS - STARTTS";
DURATION = (ENDTS - STARTTS);
;
/* Data Element Derivation (RANKELEM) */;
FORMAT RANKELEM 8.;
LABEL RANKELEM="&RL";
```

```
RANKELEM = &RANKELEM;
;
/* Data Element Derivation (RANKLBL) */;
LENGTH RANKLBL $40;
FORMAT RANKLBL $CHAR40.;
LABEL RANKLBL="LABEL OF RANKING ELEMENT";
RANKLBL = SYMGET('RL');
;
/* Data Element Derivation (NEFEVGEN) */;
LENGTH NEFEVGEN $40;
FORMAT NEFEVGEN $CHAR40.;
LABEL NEFEVGEN="GENERAL EVENT CAUSE";
NEFEVGEN = PUT(NEFGEVCC,$GENEVCD.);
;
/* Data Element Derivation (NEFEVSPC) */;
LENGTH NEFEVSPC $40;
FORMAT NEFEVSPC $CHAR40.;
LABEL NEFEVSPC="SPECIFIC EVENT CAUSE";
NEFEVSPC = PUT(NEFSEVCC,$SPCEVCD.);
;
```

USAGE CONSIDERATIONS:

All cycles are summarized together as a data range rather than reporting by individual cycle or by year, month, day, and hour as other CA MICS reports do.

3.3 MICF Inquiries

1

(SNTLDG) DAILY EVENTS RANKING BY ZONE

FIRST 10 EVENTS BY DESCENDING NUMBER OF EVENTS

NETWORK ID: NETWORK1 SYSTEM ID: SYS1 DATA RANGE: 05JULyy-01APRyy ZONE: 1

-IDENTIFICATION--	----- EVENT DESCRIPTION -----	--- FREQUENCY ---	
ELAPSED(HH:MM)	----- GENERAL CAUSE -----:---- SPECIFIC CAUSE -----	EVENTS ALERTS	
=====		=====	=====
8:51	SNALEVEL PROTOCOL	APPLICATION SUBSYSTEM	249 0
4:41	PROTOCOL-INVALID RESPONSE / COMMAND SEQ	CONTROLLER OR DEVICE	143 0
8:57	COMMUNICATIONS (LINE/MODEM/CABLE/DRIVER)	UNDETERMINED	98 7
7:32	HARDWARE OR MICROCODE	LOCAL MODEM	28 28
5:37	HARDWARE OR MICROCODE	LOCAL MODEM INTERFACE	21 21
7:21	SOFTWARE	UNDETERMINED	10 1
8:50	PROTOCOL-INVALID RESPONSE / COMMAND SEQ	SDLC DATA LINE CONTROL	10 4
8:46	HARDWARE OR SOFTWARE	UNDETERMINED	9 9
3:34	HARDWARE OR MICROCODE	DISPLAY SERVICE	3 0
0:00	SOFTWARE	IBM PROGRAM	1 0

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NEFNREVT=NUMBER OF EVENTS

RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NEF

2

```
(SNTLDG) DAILY EVENTS RANKING BY ZONE
FIRST 10 EVENTS BY DESCENDING NUMBER OF EVENTS
NETWORK ID: NETWORK1    SYSTEM ID: SYS2    DATA RANGE: 05JULyy-01APRyy    ZONE: 2
| -IDENTIFICATION-- ||----- EVENT DESCRIPTION -----||--- FREQUENCY ---|
| ELAPSED(HH:MM)   ||----- GENERAL CAUSE -----:---- SPECIFIC CAUSE -----|| EVENTS  ALERTS |
=====
18:02      PROTOCOL-INVALID RESPONSE / COMMAND SEQ SDLC DATA LINE CONTROL          279      270
16:13      COMMUNICATIONS (LINE/MODEM/CABLE/DRIVER) UNDETERMINED                    97        4
17:39      SNALEVEL PROTOCOL APPLICATION SUBSYSTEM                               69         0
2:01       PROTOCOL-INVALID RESPONSE / COMMAND SEQ CONTROLLER OR DEVICE            64         0
0:00       HARDWARE OR MICROCODE LOCAL MODEM INTERFACE                          35        25
9:55       HARDWARE OR MICROCODE DISPLAY OR PRINTER                             5         1
13:31      HARDWARE OR MICROCODE LOCAL MODEM                                    5         5
15:13      SOFTWARE UNDETERMINED                                                  2         1
0:00       HARDWARE OR MICROCODE DISPLAY SERVICE                                1         0
0:00       HARDWARE OR MICROCODE BASE PROCESSOR                                 1         1
```

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NEFNREVT=NUMBER OF EVENTS
RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NEF

3

(SNTLDG) DAILY EVENTS RANKING BY ZONE				
FIRST 10 EVENTS BY DESCENDING NUMBER OF EVENTS				
NETWORK ID: NETWORK1		SYSTEM ID: SYS3	DATA RANGE: 05JULyy-01APRyy	ZONE: 2
-IDENTIFICATION--	EVENT DESCRIPTION			FREQUENCY ---
ELAPSED(HH:MM)	GENERAL CAUSE	SPECIFIC CAUSE	EVENTS	ALERTS
0:58	SOFTWARE	UNDETERMINED	261	95
0:40	HARDWARE OR MICROCODE	DISPLAY SERVICE	51	0
0:54	HARDWARE OR MICROCODE	LOCAL MODEM INTERFACE	28	28
0:55	HARDWARE OR MICROCODE	LOCAL MODEM	27	27
0:47	HARDWARE OR SOFTWARE	MAIN STORAGE	19	19
0:49	HARDWARE OR MICROCODE	DISPLAY OR PRINTER	17	0
0:32	UNDETERMINED	UNDETERMINED	4	4
0:08	HARDWARE OR SOFTWARE	UNDETERMINED	4	3
0:11	COMMUNICATIONS (LINE/MODEM/CABLE/DRIVER)	UNDETERMINED	2	1
0:00	HARDWARE OR MICROCODE	REMOTE PRODUCT	1	1

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NEFNREVT=NUMBER OF EVENTS
RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NEF

Figure 3-

3.3.1.2.8 NetView Events by Resource Type Ranking

INTENDED USE:

To rank all events in ascending or descending order based on event frequency and resource type. The user chooses the order of ranking and resource types. The report provides both general and specific cause codes for each event listed. It is useful in identifying systems having high event activity.

FORMAT:

A 6 column report approximately 132 characters wide. It is best suited for hardcopy review but can be reviewed online. The information is summarized and presented by NETWRKID, SYSID, NEFFRTYP, NEFEVGEN, NEFEVSPC, Data Range, and Zone or Zone by Hour.

INQUIRY ID:

SNTLDI - Events/Resource types w/in zone
SNTLDJ - Events/Resource types w/in hour

DATA SOURCE (File/Timespan):

SNTNEF - Days

DATA ELEMENTS USED:

DURATION, NEFFRTYP, NEFEVGEN, NEFEVSPC, NEFNREVT, IQ,
NEFNRLT, NETWRKID, SYSID, DATA, ZONE, RANKELEM, RANKLBL,
CURRENT

CALCULATIONS:

```
/* Data Element Derivation (DATE) */;
FORMAT DATE DATE7.;
LABEL DATE="Date Selection Field";
DATE = DATEPART(ENDTS);
;
/* Data Element Derivation (TIME) */;
FORMAT TIME TIME11.2;
LABEL TIME="Time Selection Field";
TIME = TIMEPART(ENDTS);
;
/* Data Element Derivation (DATA) */;
LENGTH DATA $15;
FORMAT DATA $CHAR15.;
```

```

LABEL DATA="DATA RANGE";
DATA = ' ';
/* SAS System Statements(Derive vars & data select) */;
RETAIN DATEA DATEB;
LENGTH DATEA DATEB 4.;
DATEA = MIN(DATEA,STARTTS);
DATEB=MAX(DATEB,ENDTS);
IF _EOF_ THEN DO;
    DATEA=DATEPART(DATEA);
    DATEB=DATEPART(DATEB);
    SUBSTR(DATA,1,7)=PUT(DATEA,DATE7.);
    SUBSTR(DATA,8,1)='- ';
    SUBSTR(DATA,9,7)=PUT(DATEB,DATE7.);
    CALL SYMPUT('S',DATA);
    %GLOBAL S;
    DROP DATEA DATEB;
END;
/* Data Summarization */
%MACRO NEGATE;
    DATA=SYMGET('S');
%MEND NEGATE;
;
/* Data Element Derivation (CURRENT, &C) */;
FORMAT CURRENT WEEKDATE15.;
LABEL CURRENT="CURRENT DATE";
CURRENT = TODAY();
C=PUT(CURRENT,WEEKDATE15.);
C=COMPRESS(C) ;
CALL SYMPUT('C',PUT(C,$CHAR12.));
%GLOBAL C;
;
/* Data Element Derivation (IQ, &I) */;
LENGTH IQ $8;
FORMAT IQ $CHAR8.;
LABEL IQ="Inquire Name";
IQ = ' ';
SUBSTR(IQ,1,1)='(';
SUBSTR(IQ,2,6)=SYMGET('INQINAME');
SUBSTR(IQ,8,1)=')';
CALL SYMPUT('I',PUT(IQ,$CHAR8.));
%GLOBAL I;
;
/* Data Element Derivation (DURATION, elapsed time) */;
FORMAT DURATION TIME5.2;
LABEL DURATION="ENDTS - STARTTS";
DURATION = (ENDTS - STARTTS);
;
/* Data Element Derivation (RANKELEM) */;
FORMAT RANKELEM 8.;

```

```
LABEL RANKELEM="&RL";
RANKELEM = &RANKELEM;
;
/* Data Element Derivation (RANKLBL) */;
LENGTH RANKLBL $40;
FORMAT RANKLBL $CHAR40.;
LABEL RANKLBL="LABEL OF RANKING ELEMENT";
RANKLBL = SYMGET('RL');
;
/* Data Element Derivation (NEFEVGEN) */;
LENGTH NEFEVGEN $40;
FORMAT NEFEVGEN $CHAR40.;
LABEL NEFEVGEN="GENERAL EVENT CAUSE";
NEFEVGEN = PUT(NEFGEVCC,$GENEVCD.);
;
/* Data Element Derivation (NEFEVSPC) */;
LENGTH NEFEVSPC $40;
FORMAT NEFEVSPC $CHAR40.;
LABEL NEFEVSPC="SPECIFIC EVENT CAUSE";
NEFEVSPC = PUT(NEFSEVCC,$SPCEVCD.);
;
```

USAGE CONSIDERATIONS:

All cycles are summarized together as a data range, rather than reporting by an individual cycle or by year, month, day, and hour, as other CA MICS reports do.

1

```

(SNTLDI) DAILY FAILING RESOURCE TYPE RANKING BY ZONE
FIRST 10 RESOURCE TYPES BY DESCENDING NUMBER OF EVENTS
NETWORK ID: NETWORK1  SYSTEM ID: SYS1  DATA RANGE: 05JULyy-01APRyy  ZONE: 1
| -IDENTIFICATION-- ||----- EVENT DESCRIPTION -----||--- FREQUENCY ---|
| ELAPSED(HH:MM) / ||----- GENERAL CAUSE -----:---- SPECIFIC CAUSE -----|| EVENTS  ALERTS |
| RESOURCE TYPE  ||-----||-----||-----||-----|
=====
8:51  DEV  SNALEVEL PROTOCOL          APPLICATION SUBSYSTEM          217      0
4:41  CTRL  PROTOCOL-INVALID RESPONSE / COMMAND SEQ  CONTROLLER OR DEVICE         143      0
8:57  CTRL  COMMUNICATIONS (LINE/MODEM/CABLE/DRIVER)  UNDETERMINED                  86       4
8:14  LDEV  SNALEVEL PROTOCOL          APPLICATION SUBSYSTEM          32       0
7:32  LINE  HARDWARE OR MICROCODE        LOCAL MODEM                   28      28
5:37  LINE  HARDWARE OR MICROCODE        LOCAL MODEM INTERFACE         21      21
7:21  CTRL  SOFTWARE                     UNDETERMINED                  10       1
8:50  CTRL  PROTOCOL-INVALID RESPONSE / COMMAND SEQ  SDLC DATA LINE CONTROL      10       4
7:03  LINE  COMMUNICATIONS (LINE/MODEM/CABLE/DRIVER)  UNDETERMINED                  10       2
8:46  CTRL  HARDWARE OR SOFTWARE          UNDETERMINED                   9       9

```

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NEFNREVT=NUMBER OF EVENTS
 RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NEF

2

```

(SNTLDI) DAILY FAILING RESOURCE TYPE RANKING BY ZONE
FIRST 10 RESOURCE TYPES BY DESCENDING NUMBER OF EVENTS
NETWORK ID: NETWORK1  SYSTEM ID: SYS2  DATA RANGE: 05JULyy-01APRyy  ZONE: 2
| -IDENTIFICATION-- ||----- EVENT DESCRIPTION -----||--- FREQUENCY ---|
| ELAPSED(HH:MM) / ||----- GENERAL CAUSE -----:---- SPECIFIC CAUSE -----|| EVENTS  ALERTS |
| RESOURCE TYPE  ||-----||-----||-----||-----|
=====
18:02 CTRL  PROTOCOL-INVALID RESPONSE / COMMAND SEQ  SDLC DATA LINE CONTROL      279     270
16:13 CTRL  COMMUNICATIONS (LINE/MODEM/CABLE/DRIVER)  UNDETERMINED                  94       3
2:01  CTRL  PROTOCOL-INVALID RESPONSE / COMMAND SEQ  CONTROLLER OR DEVICE         64       0
17:05 LDEV  SNALEVEL PROTOCOL          APPLICATION SUBSYSTEM          44       0
0:00  LINE  HARDWARE OR MICROCODE        LOCAL MODEM INTERFACE         35      25
17:06 DEV  SNALEVEL PROTOCOL          APPLICATION SUBSYSTEM          25       0
9:55  DEV  HARDWARE OR MICROCODE        DISPLAY OR PRINTER            5        1
13:31 LINE  HARDWARE OR MICROCODE        LOCAL MODEM                    5        5
15:13 CTRL  SOFTWARE                     UNDETERMINED                   2        1
0:05  LINE  COMMUNICATIONS (LINE/MODEM/CABLE/DRIVER)  UNDETERMINED                   2        1

```

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NEFNREVT=NUMBER OF EVENTS
 RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NEF

```

(SNTLDI) DAILY FAILING RESOURCE TYPE RANKING BY ZONE
FIRST 10 RESOURCE TYPES BY DESCENDING NUMBER OF EVENTS
NETWORK ID: NETWORK1  SYSTEM ID: SYS3  DATA RANGE: 05JULyy-01APRyy  ZONE: 2
| IDENTIFICATION | |-----| EVENT DESCRIPTION | |---| FREQUENCY |---|
| ELAPSED(HH:MM) / | |-----| GENERAL CAUSE |-----| SPECIFIC CAUSE |-----| | EVENTS | ALERTS |
| RESOURCE TYPE | | | | | | | |
=====
0:58  DEV    SOFTWARE          UNDETERMINED          129      0
0:57  CTRL   SOFTWARE          UNDETERMINED          88      62
0:40  DEV    HARDWARE OR MICROCODE  DISPLAY SERVICE       51      0
0:21  LKST   SOFTWARE          UNDETERMINED          33      33
0:54  LINE   HARDWARE OR MICROCODE  LOCAL MODEM INTERFACE  28      28
0:55  LINE   HARDWARE OR MICROCODE  LOCAL MODEM           27      27
0:47  CTRL   HARDWARE OR SOFTWARE   MAIN STORAGE           19      19
0:49  DEV    HARDWARE OR MICROCODE  DISPLAY OR PRINTER     17      0
0:56  LINE   SOFTWARE          UNDETERMINED          11      0
0:32  CTRL   UNDETERMINED          UNDETERMINED           4       4

```

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NEFNREVT=NUMBER OF EVENTS
 RUN-DATE=Wed,Sep3,yy, TIMESPAN=DAYS, DBID=8, FILE=NEF

Figure 3-

3.3.1.2.9 NetView Events by Resource Ranking

INTENDED USE:

To rank all events in ascending or descending order based on event frequency by resource name. The user chooses the order of ranking. The report provides both general and specific cause codes for each event listed. It is useful in identifying resources having high event activity.

FORMAT:

A 6 column report approximately 132 characters wide. It is best suited for hardcopy review but can be reviewed online. The information is summarized and presented by NETWRKID, SYSID, NEFFRNAM, NEFEVGEN, NEFEVSPC, Data Range, and Zone or Zone by Hour.

INQUIRY ID:

SNTLDO - Events/Resources w/in zone

SNTLDP - Events/Resources w/in hour

DATA SOURCE (File/Timespan):

SNTNEF - Days

DATA ELEMENTS USED:

DURATION, NEFFRNAM, NEFEVGEN, NEFEVSPC, NEFNREVT, IQ, NEFNRLT, NETWRKID, SYSID, DATA, ZONE, RANKELEM, RANKLBL, CURRENT

CALCULATIONS:

```
/* Data Element Derivation (DATE) */;
FORMAT DATE DATE7.;
LABEL DATE="Date Selection Field";
DATE = DATEPART(ENDTS);
;
/* Data Element Derivation (TIME) */;
FORMAT TIME TIME11.2;
LABEL TIME="Time Selection Field";
TIME = TIMEPART(ENDTS);
;
/* Data Element Derivation (DATA) */;
LENGTH DATA $15;
FORMAT DATA $CHAR15.;
```

```

LABEL DATA="DATA RANGE";
DATA = ' ';
/* SAS System Statements(Derive vars & data select) */;
RETAIN DATEA DATEB;
LENGTH DATEA DATEB 4.;
DATEA = MIN(DATEA,STARTTS);
DATEB=MAX(DATEB,ENDTS);
IF _EOF_ THEN DO;
    DATEA=DATEPART(DATEA);
    DATEB=DATEPART(DATEB);
    SUBSTR(DATA,1,7)=PUT(DATEA,DATE7.);
    SUBSTR(DATA,8,1)='- ';
    SUBSTR(DATA,9,7)=PUT(DATEB,DATE7.);
    CALL SYMPUT('S',DATA);
    %GLOBAL S;
    DROP DATEA DATEB;
END;
/* Data Summarization */
%MACRO NEGATE;
    DATA=SYMGET('S');
%MEND NEGATE;
;
/* Data Element Derivation (CURRENT, &C) */;
FORMAT CURRENT WEEKDATE15.;
LABEL CURRENT="CURRENT DATE";
CURRENT = TODAY();
C=PUT(CURRENT,WEEKDATE15.);
C=COMPRESS(C) ;
CALL SYMPUT('C',PUT(C,$CHAR12.));
%GLOBAL C;
;
/* Data Element Derivation (IQ, &I) */;
LENGTH IQ $8;
FORMAT IQ $CHAR8.;
LABEL IQ="Inquire Name";
IQ = ' ';
SUBSTR(IQ,1,1)='(';
SUBSTR(IQ,2,6)=SYMGET('INQINAME');
SUBSTR(IQ,8,1)=')';
CALL SYMPUT('I',PUT(IQ,$CHAR8.));
%GLOBAL I;
;
/* Data Element Derivation (DURATION, elapsed time) */;
FORMAT DURATION TIME5.2;
LABEL DURATION="ENDTS - STARTTS";
DURATION = (ENDTS - STARTTS);
;
/* Data Element Derivation (RANKELEM) */;
FORMAT RANKELEM 8.;
```



```

LABEL RANKELEM="&RL";
RANKELEM = &RANKELEM;
;
/* Data Element Derivation (RANKLBL) */;
LENGTH RANKLBL $40;
FORMAT RANKLBL $CHAR40.;
LABEL RANKLBL="LABEL OF RANKING ELEMENT";
RANKLBL = SYMGET('RL');
;
/* Data Element Derivation (NEFEVGEN) */;
LENGTH NEFEVGEN $40;
FORMAT NEFEVGEN $CHAR40.;
LABEL NEFEVGEN="GENERAL EVENT CAUSE";
NEFEVGEN = PUT(NEFGEVCC,$GENEVCD.);
;
/* Data Element Derivation (NEFEVSPC) */;
LENGTH NEFEVSPC $40;
FORMAT NEFEVSPC $CHAR40.;
LABEL NEFEVSPC="SPECIFIC EVENT CAUSE";
NEFEVSPC = PUT(NEFSEVCC,$SPCEVCD.);
;

```

USAGE CONSIDERATIONS:

All cycles are summarized together as a data range rather than reporting by individual cycle or by year, month, day, and hour as other CA MICS reports do.

3.3 MICF Inquiries

1

(SNTLDO) DAILY FAILING RESOURCE NAME RANKING BY ZONE

FIRST 10 RESOURCE NAMES BY DESCENDING NUMBER OF EVENTS

NETWORK ID: NETWORK1 SYSTEM ID: SYS1 DATA RANGE: 05JULyy-01APRyy ZONE: 1

-IDENTIFICATION--		----- EVENT DESCRIPTION -----		--- FREQUENCY ---	
ELAPSED(HH:MM) /		----- GENERAL CAUSE -----:----- SPECIFIC CAUSE -----		EVENTS ALERTS	
RESOURCE NAME					
=====				=====	
4:41	P260047	PROTOCOL-INVALID RESPONSE / COMMAND SEQ	CONTROLLER OR DEVICE	142	0
0:02	T2601029	SNALEVEL PROTOCOL	APPLICATION SUBSYSTEM	19	0
7:28	T3600935	SNALEVEL PROTOCOL	APPLICATION SUBSYSTEM	19	0
6:22	H0411024	SNALEVEL PROTOCOL	APPLICATION SUBSYSTEM	18	0
1:26	P230165	COMMUNICATIONS (LINE/MODEM/CABLE/DRIVER)	UNDETERMINED	16	0
5:33	T3600932	SNALEVEL PROTOCOL	APPLICATION SUBSYSTEM	16	0
4:46	T2306341	SNALEVEL PROTOCOL	APPLICATION SUBSYSTEM	15	0
0:15	L23L016	HARDWARE OR MICROCODE	LOCAL MODEM INTERFACE	13	13
7:40	P230137	COMMUNICATIONS (LINE/MODEM/CABLE/DRIVER)	UNDETERMINED	13	0
0:02	T2306361	SNALEVEL PROTOCOL	APPLICATION SUBSYSTEM	13	0

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NEFNREVT=NUMBER OF EVENTS

RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NEF

2

```
(SNTLD0) DAILY FAILING RESOURCE NAME RANKING BY ZONE
FIRST 10 RESOURCE NAMES BY DESCENDING NUMBER OF EVENTS
NETWORK ID: NETWORK1    SYSTEM ID: SYS2    DATA RANGE: 05JULyy-01APRyy    ZONE: 2

|-IDENTIFICATION--| |----- EVENT DESCRIPTION -----| |--- FREQUENCY ---|
|ELAPSED(HH:MM) / | |----- GENERAL CAUSE -----:----- SPECIFIC CAUSE -----| |EVENTS  ALERTS |
| RESOURCE NAME  | |                                     | |          |
=====
6:57  P230008  PROTOCOL-INVALID RESPONSE / COMMAND SEQ SDLC DATA LINE CONTROL          269      269
2:01  P260047  PROTOCOL-INVALID RESPONSE / COMMAND SEQ CONTROLLER OR DEVICE                64        0
3:29  P230165  COMMUNICATIONS (LINE/MODEM/CABLE/DRIVER) UNDETERMINED                       23        0
0:35  H0411024  SNALLEVEL PROTOCOL APPLICATION SUBSYSTEM                                16        0
0:02  H0411537  SNALLEVEL PROTOCOL APPLICATION SUBSYSTEM                                16        0
0:13  P230163  COMMUNICATIONS (LINE/MODEM/CABLE/DRIVER) UNDETERMINED                       6         1
0:09  P230169  COMMUNICATIONS (LINE/MODEM/CABLE/DRIVER) UNDETERMINED                       5         0
0:00  H0411538  SNALLEVEL PROTOCOL APPLICATION SUBSYSTEM                                4         0
10:39 P230097  COMMUNICATIONS (LINE/MODEM/CABLE/DRIVER) UNDETERMINED                       4         1
0:29  H0411582  SNALLEVEL PROTOCOL APPLICATION SUBSYSTEM                                3         0

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NEFNREVT=NUMBER OF EVENTS
RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NEF
```

3

(SNTLDO) DAILY FAILING RESOURCE NAME RANKING BY ZONE												
FIRST 10 RESOURCE NAMES BY DESCENDING NUMBER OF EVENTS												
NETWORK ID: NETWORK1		SYSTEM ID: SYS3		DATA RANGE: 05JULyy-01APRyy			ZONE: 2					
-IDENTIFICATION--		----- EVENT DESCRIPTION -----					--- FREQUENCY ---					
ELAPSED(HH:MM) /		----- GENERAL CAUSE -----		----- SPECIFIC CAUSE -----			EVENTS ALERTS					
RESOURCE NAME												
=====							=====					
0:21	C108098A	SOFTWARE	UNDETERMINED				24	24				
0:36	CB67002	SOFTWARE	UNDETERMINED				19	19				
0:55	1538AU	SOFTWARE	UNDETERMINED				18	0				
0:55	2840B6	SOFTWARE	UNDETERMINED				15	0				
0:49	A0327380	HARDWARE OR MICROCODE	DISPLAY OR PRINTER				14	0				
0:53	1724Y1	SOFTWARE	UNDETERMINED				12	0				
0:26	A0131842	HARDWARE OR MICROCODE	DISPLAY SERVICE				11	0				
0:14	A0131845	HARDWARE OR MICROCODE	DISPLAY SERVICE				11	0				
0:26	A0131849	HARDWARE OR MICROCODE	DISPLAY SERVICE				11	0				
0:26	A0131852	HARDWARE OR MICROCODE	DISPLAY SERVICE				11	0				

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NEFNREVT=NUMBER OF EVENTS
RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NEF

3.3.1.2.10 NPDA Daily Resource Alert Summary

INTENDED USE:

Ranks all alerts (both standard and generic) in descending order based on alert frequency by resource name to identify the resources with the highest frequency of alerts. To the NetView Hardware Monitor, an alert indicates a problem that requires operator attention.

FORMAT:

A 3 column report approximately 132 characters wide. It is best suited for hardcopy review, but you can also review the report online. The information is summarized and presented by NETWRKID, SNTFRNAM, SNTFRTYP, Data Range, and Zone.

INQUIRY ID:

SNTLDT - NPDA Daily Resource Alert Summary

DATA SOURCE (Files/Timespan):

SNTNEF, SNTNSF, SNTLNF, SNTGAF - Days

DATA ELEMENTS USED:

ENDTS, STARTTS, SNTFRNAM, SNTFRTYP, SNTNRALT, SNTFRNM1, SNTFRNM2, SNTFRNM3, SNTFRNM4, SNTFRTY1, SNTFRTY2, SNTFRTY3, SNTFRTY4, NETWRKID, ZONE

CALCULATIONS:

None

USAGE CONSIDERATIONS:

All cycles are summarized together as a data range rather than reported by individual cycle or by year, month, day, and zone as other CA MICS reports do.

NPDA Daily Resource Alert Summary										1
INQUIRY: SNTLDT										
Net ID: NETWORK1 Zone: 1 Data Range: FROM 040CTyy:14:01:36 TO 05JULyy:16:59:51										RUN DATE: 03SEPyy
RESOURCE NAME	TYPE	NAME1	TYPE1	NAME2	TYPE2	NAME3	TYPE3	NAME4	TYPE4	TOTAL ALERTS
L23L016	LINE	N23WICB	COMC	L23L016	LINE					14
L28L019	LINE	N28NCCI	COMC	L28L019	LINE					11
L23L028	LINE	N23WICB	COMC	L23L028	LINE					9
P230008	CTRL	N23WICB	COMC	L23L008	LINE	P230008	CTRL			5
P360036A	CTRL	LMF36BN	COMC	L36L036	LINE	P360036A	CTRL			5
L28L055	LINE	N28NCCI	COMC	L28L055	LINE					3
L28L058	LINE	N28NCCI	COMC	L28L058	LINE					3
L25L042	LINE	N25NCCF	COMC	L25L042	LINE					2
L28L056	LINE	N28NCCI	COMC	L28L056	LINE					2
PS2I2	DEV	SRT37273	CP	PS2I2	DEV					2

2

NPDA Daily Resource Alert Summary

INQUIRY: SNTLDT

Net ID: NETWORK1 Zone: 2 Data Range: FROM 05JULyy:05:56:44 TO 01APRyy:23:59:58

RUN DATE: 03SEPyy

RESOURCE NAME	TYPE	NAME1	TYPE1	NAME2	TYPE2	NAME3	TYPE3	NAME4	TYPE4	TOTAL ALERTS
P230008	CTRL	N23WICB	COMC	L23L008	LINE	P230008	CTRL			269
TAP01	TAPE	A0329542	CP	CMB01	LCTL	DC03	ADPT	TAP01	TAPE	32
A0335745	RC2N	A0335745	RC2N							27
A0328663	RC2N	A0328663	RC2N							26
A0329554	RC2N	A0329554	RC2N							26
C108098A	LKST	N108L6	COMC	L108083	LINE	C108098	CTRL	C1080980	LINE	24
H04222P	CTRL	N24NCCE	COMC	J0000013	LINE	H04222P	CTRL			22
CB67002	CTRL	PUSB67	COMC	LB67080	LINE	CB67002	CTRL			19
N002L4	COMC	N002L4	COMC							17
CD24000	CTRL	PUSD24	COMC	LD24080	LINE	CD24000	CTRL			15

Figure 3-

3.3.1.2.11 NPDA Daily Resource Alert Description

INTENDED USE:

To identify the 10 resources with the greatest number of alerts (both standard and generic) and to sum total alerts by alert description for each of these resources. To the NetView Hardware Monitor, an alert indicates a problem that requires operator attention.

FORMAT:

A 3 column report approximately 132 characters wide. It is best suited for hardcopy review, but you can also review the report online. The information is summarized and presented by NETWRKID, SNTFRNAM, SNTFRTYP, Alert Description, NETWRKID, SNTFRNAM, SNTFRTYP, Data Range, and Zone.

INQUIRY ID:

SNTLDU - Daily NPDA Resource Alert Description

DATA SOURCE (Files/Timespan):

SNTNEF, SNTNSF, SNTLNF, SNTGAF - Days

DATA ELEMENTS USED:

ENDTS, STARTTS, SNTFRNAM, SNTFRTYP, SNTNRALT, SNTFRNM1, SNTFRNM2, SNTFRTY1, SNTFRTY2, SNTGADSC, SNTERRDS, NETWRKID, ZONE

CALCULATIONS:

None

USAGE CONSIDERATIONS:

All cycles are summarized together as a data range rather than reported by individual cycle or by year, month, day, and zone as other CA MICS reports do.

3.3 MICF Inquiries

NPDA Daily Resource Alert Description										
INQUIRY: SNTLDU						Net ID: NETWORK1 Zone: 1 Data Range: FROM 05JULyy:08:02:59 TO 05JULyy:16:59:39				
						RUN DATE: 03SEPyy				
RESOURCE NAME	TYPE	NAME1	TYPE1	NAME2	TYPE2	ALERT TYPE	PROB TYPE	PROBLEM DESCRIPTION	DESC TOTAL	RESOURCE TOTAL
L23L016	LINE	N23WICB	COMC	L23L016	LINE	STANDARD	PERM DSR ON CHECK:LOCAL MODEM OFF/LOCAL MODEM		13	14
						STANDARD	PERM MODEM ERROR:LOCAL MODEM OFF/LOCAL MODEM		1	
L28L019	LINE	N28NCCI	COMC	L28L019	LINE	STANDARD	PERM MODEM ERROR:LOCAL MODEM OFF/LOCAL MODEM		10	11
						STANDARD	PERM DSR ON CHECK:LOCAL MODEM OFF/LOCAL MODEM		1	
L23L028	LINE	N23WICB	COMC	L23L028	LINE	STANDARD	PERM DSR ON CHECK:LOCAL MODEM OFF/LOCAL MODEM		7	9
						STANDARD	PERM MODEM ERROR:LOCAL MODEM OFF/LOCAL MODEM		2	
P230008	CTRL	N23WICB	COMC	L23L008	LINE	STANDARD	PERM FORMAT EXCEPTION:DEVICE		4	5
						STANDARD	PERM TIMEOUT:DEVICE OFF/REMOTE MODEM OFF/COMM		1	
						STATISTIC	N/A EXCESSIVE TRAFFIC, ERRORS, OR ERROR/TRAFFIC RATIO		0	
P360036A	CTRL	LMF36BN	COMC	L36L036	LINE	STANDARD	PERM REQUEST DISCONNECT RECEIVED:REMOTE DEVICE		5	5
						STATISTIC	N/A EXCESSIVE TRAFFIC, ERRORS, OR ERROR/TRAFFIC RATIO		0	
L28L055	LINE	N28NCCI	COMC	L28L055	LINE	STANDARD	PERM MODEM ERROR:LOCAL MODEM OFF/LOCAL MODEM		3	3
L28L058	LINE	N28NCCI	COMC	L28L058	LINE	STANDARD	PERM MODEM ERROR:LOCAL MODEM OFF/LOCAL MODEM		3	3
						STATISTIC	N/A EXCESSIVE TRAFFIC, ERRORS, OR ERROR/TRAFFIC RATIO		0	
L25L042	LINE	N25NCCF	COMC	L25L042	LINE	STANDARD	PERM MODEM ERROR:LOCAL MODEM OFF/LOCAL MODEM		2	2
						STATISTIC	N/A EXCESSIVE TRAFFIC, ERRORS, OR ERROR/TRAFFIC RATIO		0	
L28L056	LINE	N28NCCI	COMC	L28L056	LINE	STANDARD	PERM MODEM ERROR:LOCAL MODEM OFF/LOCAL MODEM		2	2
						STATISTIC	N/A EXCESSIVE TRAFFIC, ERRORS, OR ERROR/TRAFFIC RATIO		0	
PS2I2	DEV	SRT37273	CP	PS2I2	DEV	STATISTIC	N/A EXCESSIVE TRAFFIC, ERRORS, OR ERROR/TRAFFIC RATIO		2	2

NPDA Daily Resource Alert Description										
INQUIRY: SNTLDU										
Net ID: NETWORK1 Zone: 2 Data Range: FROM 05JULyy:05:56:54 TO 01APRyy:23:59:11										
RUN DATE: 03SEPyy										
RESOURCE NAME	TYPE	NAME1	TYPE1	NAME2	TYPE2	ALERT TYPE	PROB TYPE	PROBLEM DESCRIPTION	DESC TOTAL	RESOURCE TOTAL
P230008	CTRL	N23WICB	COMC	L23L008	LINE	STANDARD	PERM	FORMAT EXCEPTION:DEVICE	269	269
						STATISTIC	N/A	EXCESSIVE TRAFFIC, ERRORS, OR ERROR/TRAFFIC RATIO	0	
TAP01	TAPE	A0329542	CP	CMB01	LCTL	STANDARD	PERM	EXCESSIVE TRAFFIC, ERRORS, OR ERROR/TRAFFIC RATIO	30	32
						STATISTIC	N/A	EXCESSIVE TRAFFIC, ERRORS, OR ERROR/TRAFFIC RATIO	2	
A0335745	RC2N	A0335745	RC2N			STANDARD	PERM	EXCESSIVE TRAFFIC, ERRORS, OR ERROR/TRAFFIC RATIO	27	
						STATISTIC	N/A	EXCESSIVE TRAFFIC, ERRORS, OR ERROR/TRAFFIC RATIO	27	
A0328663	RC2N	A0328663	RC2N			STANDARD	PERM	EXCESSIVE TRAFFIC, ERRORS, OR ERROR/TRAFFIC RATIO	26	
						STATISTIC	N/A	EXCESSIVE TRAFFIC, ERRORS, OR ERROR/TRAFFIC RATIO	26	
A0329554	RC2N	A0329554	RC2N			STANDARD	PERM	EXCESSIVE TRAFFIC, ERRORS, OR ERROR/TRAFFIC RATIO	26	
						STATISTIC	N/A	EXCESSIVE TRAFFIC, ERRORS, OR ERROR/TRAFFIC RATIO	26	
C108098A	LKST	N108L6	COMC	L108083	LINE	STANDARD	PROC	SERIES/1 ALERT; TYPE= SCIM APPLICATION	24	24
H04222P	CTRL	N24NCCE	COMC	J0000013	LINE	STANDARD	PERM	OUTGOING CALL REFUSED:PHYSICAL LINK DOWN	21	22
						STANDARD	PERM	NO DATA RECEIVED:DEVICE OFF/COMM	1	
CB67002	CTRL	PUSB67	COMC	LB67080	LINE	STANDARD	PROC	SERIES/1 ALERT; TYPE= SCIM APPLICATION	19	19
N002L4	COMC	N002L4	COMC			STANDARD	PERM	EXCESSIVE TRAFFIC, ERRORS, OR ERROR/TRAFFIC RATIO	17	
						STATISTIC	N/A	EXCESSIVE TRAFFIC, ERRORS, OR ERROR/TRAFFIC RATIO	17	
CD24000	CTRL	PUSD24	COMC	LD24080	LINE	STANDARD	PERM	EXCESSIVE TRAFFIC, ERRORS, OR ERROR/TRAFFIC RATIO	15	15
						STATISTIC	N/A	EXCESSIVE TRAFFIC, ERRORS, OR ERROR/TRAFFIC RATIO	15	

Figure 3-

3.3.1.2.12 NPDA Detail Generic Alert Report

INTENDED USE:

To provide detailed descriptions of generic alerts for resources selected by the client.

FORMAT:

A 3 column report approximately 132 characters wide. It is best suited for hardcopy review, but you can also review the report online. The information is summarized and presented by NETWRKID, ZONE, and SNTFTNAM.

INQUIRY ID:

SNTLDV - NPDA Detail Generic Alert Report

DATA SOURCE (Files/Timespan):

SNTGAF - Detail

DATA ELEMENTS USED:

ENDTS, STARTTS, SNTFRNAM, SNFRFTYP, SNTTEVTS, SNTGAID, ZONE SNTGADSC, SNT1PRBC, SNTTEVNT, NETWRKID

CALCULATIONS:

None

USAGE CONSIDERATIONS:

All cycles are summarized together as a data range rather than reported by individual cycle or by year, month, day, and zone as other CA MICS reports do.

NPDA Detail Generic Alert Report					1
INQUIRY: SNTLDV					
Net ID: NETWORK1 Zone: 1 Domain: NET04 Resource Name: CTL01000					RUN DATE: 03SEPyy
Resource Type	Event Timestamp	Event Type	Alert ID	Generic Alert Description	
PRT	05JULyy:09:54:18.00	TEMP PRINTER	40AC07EA	OPERATOR INTERVENTION REQUIRED	
PRT	05JULyy:11:50:17.00	TEMP PRINTER	40AC07EA	OPERATOR INTERVENTION REQUIRED	
PRT	05JULyy:11:51:47.00	TEMP PRINTER	40AC07EA	OPERATOR INTERVENTION REQUIRED	
PRT	05JULyy:11:52:57.00	TEMP PRINTER	40AC07EA	OPERATOR INTERVENTION REQUIRED	
PRT	05JULyy:11:53:39.00	TEMP PRINTER	40AC07EA	OPERATOR INTERVENTION REQUIRED	
PRT	05JULyy:11:53:46.00	TEMP PRINTER	40AC07EA	OPERATOR INTERVENTION REQUIRED	
PRT	05JULyy:11:54:29.00	TEMP PRINTER	40AC07EA	OPERATOR INTERVENTION REQUIRED	
PRT	05JULyy:11:59:14.00	TEMP PRINTER	40AC07EA	OPERATOR INTERVENTION REQUIRED	
PRT	05JULyy:12:00:24.00	TEMP PRINTER	40AC07EA	OPERATOR INTERVENTION REQUIRED	
PRT	05JULyy:12:01:25.00	TEMP PRINTER	40AC07EA	OPERATOR INTERVENTION REQUIRED	
PRT	05JULyy:12:02:28.00	TEMP PRINTER	40AC07EA	OPERATOR INTERVENTION REQUIRED	

Figure 3-

3.3.1.2.13 NPDA Daily Alerts by Problem Type

INTENDED USE:

This chart is used to show both the count and percentage of generic and standard alerts (detected by the NetView Hardware Monitor) by problem type for each zone.

FORMAT:

This display produces a pie chart of total alerts grouped by alert type (e.g., permanent, performance, or temporary) for all resources for each zone, and for the time period specified in the data range.

INQUIRY ID:

Color Graphics: SNTCDL
Printer Graphics: SNTPDL

DATA SOURCE (Files/Timespan):

SNTNEF, SNTNSF, SNTLNF, SNTGAF - Days

DATA ELEMENTS USED:

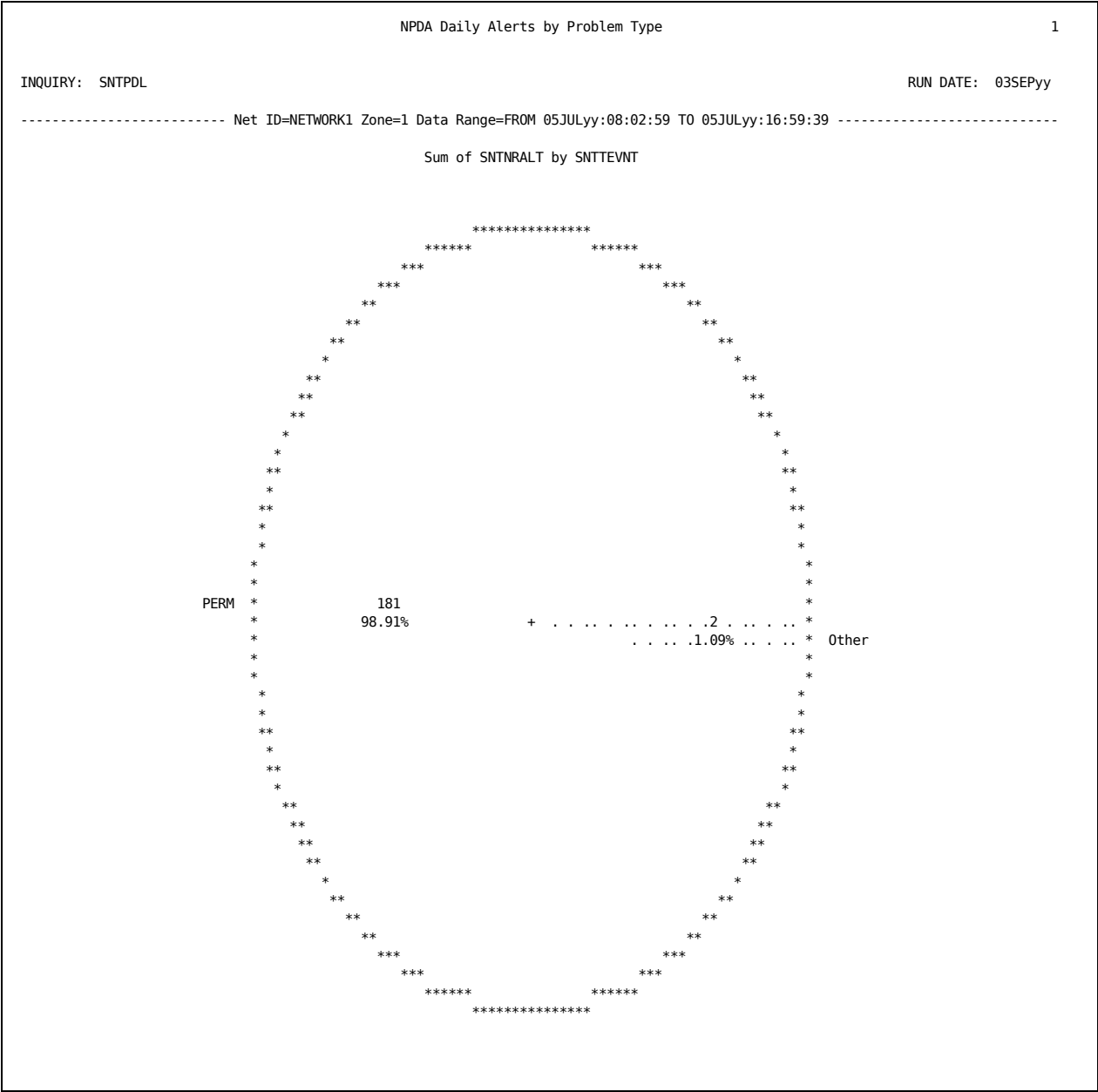
SNTTEVNT, SNTNRALT, STARTTS, ENDTS, ZONE

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This inquiry is produced from NetView Hardware Monitor data only.



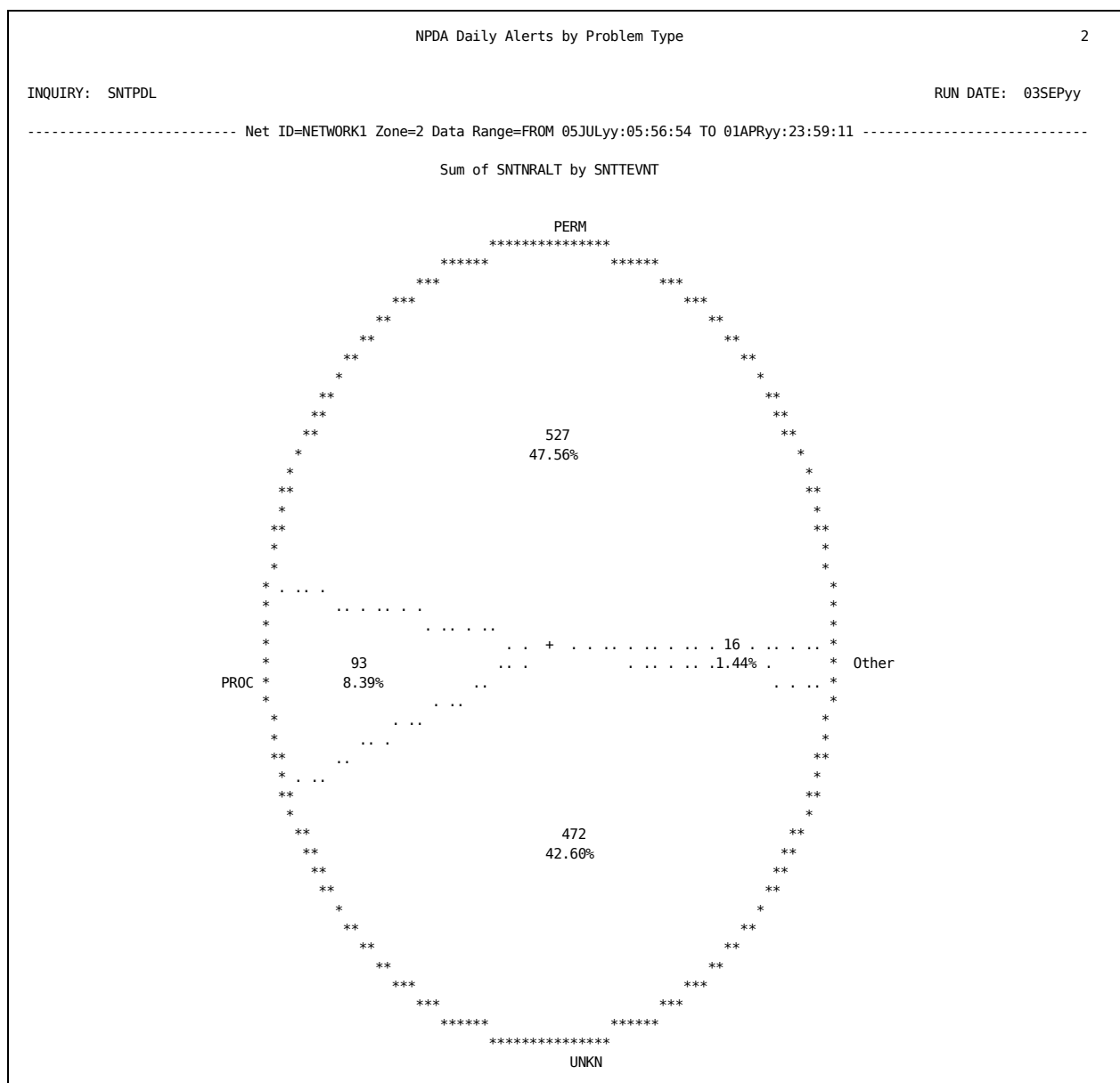


Figure 3-

3.3.1.2.14 NPDA Daily Alerts by Resource Type

INTENDED USE:

This chart is used to show both the count and percentage of generic and standard alerts (detected by the NetView Hardware Monitor) by resource type for each zone.

FORMAT:

This display produces a pie chart of total alerts grouped by resource type (e.g., controller, line, LU) for each zone for the time period specified in the data range.

INQUIRY ID:

Color Graphics: SNTCDM
Printer Graphics: SNTPDM

DATA SOURCE (Files/Timespan):

SNTNEF, SNTNSF, SNTLNF, SNTGAF - Days

DATA ELEMENTS USED:

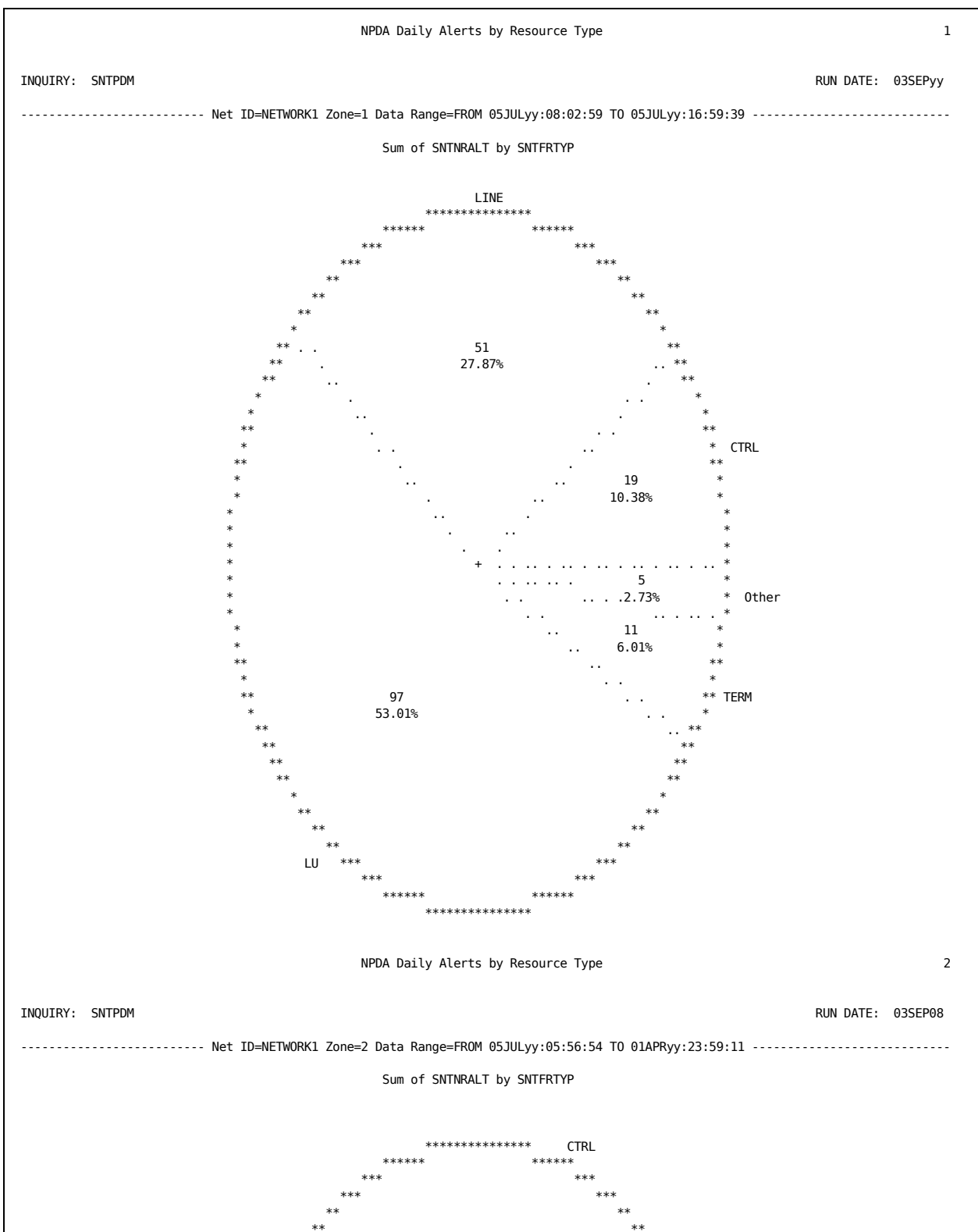
SNTFRTYP, SNTNRALT, STARTTS, ENDTS, ZONE

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This inquiry is produced from NetView Hardware Monitor data only.



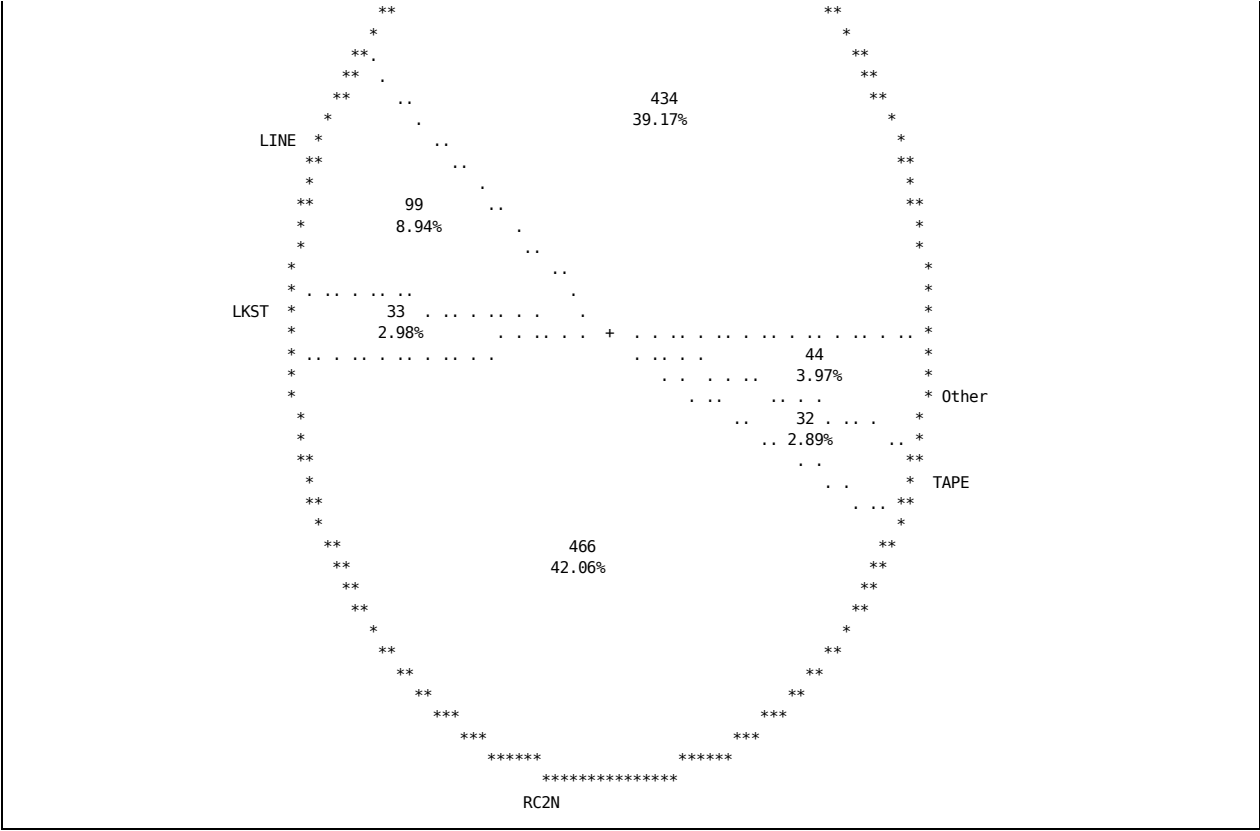


Figure 3-

3.3.1.3 Performance Analysis Inquiries

Performance analysis inquiries indicate daily performance by hour of NCPs and links. These inquiries are explained in greater detail in the following sections:

- 1 - NPM Daily Pct. NCP Cycle Utilization
- 2 - NPM Daily NCP Buffer Utilization
- 3 - NPM Daily Link Utilization
- 4 - NetSpy Daily Pct. NCP Cycle Utilization
- 5 - NetSpy Daily NCP Buffer Utilization
- 6 - NetSpy Daily Link Utilization
- 7 - NCP Utilization Ranking
- 8 - NCP Utilization Chart
- 9 - NCP Utilization Plot
- 10 - NCP Channel Hold/Intermediate Queue Length Plot
- 11 - NetSpy Daily Average VR Response Time
- 12 - NetSpy Daily Pct. Time VR Held/Blocked
- 13 - Under/Over Utilized Line Analysis
- 14 - NPM/NetSpy Link Ranking By (Zone/Hour)
- 15 - NPM/NetSpy Daily Link Utilization

3.3.1.3.1 NPM Daily Pct. NCP Cycle Utilization

INTENDED USE:

This chart is used to determine the communications processor load variation (communications controller utilization cycles) over a period of 24 hours.

FORMAT:

This display produces a vertical bar chart of communications controller processor percentage utilization by hour.

INQUIRY ID:

Color Graphics: SNTCD6
Printer Graphics: SNTPD6

DATA SOURCE (File/Timespan):

SNTNAF01 - Previous day

DATA ELEMENTS USED:

HOURL, NAFPCCU, NCPNAME

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This inquiry is produced from NetView Performance Monitor (NPM) network data.

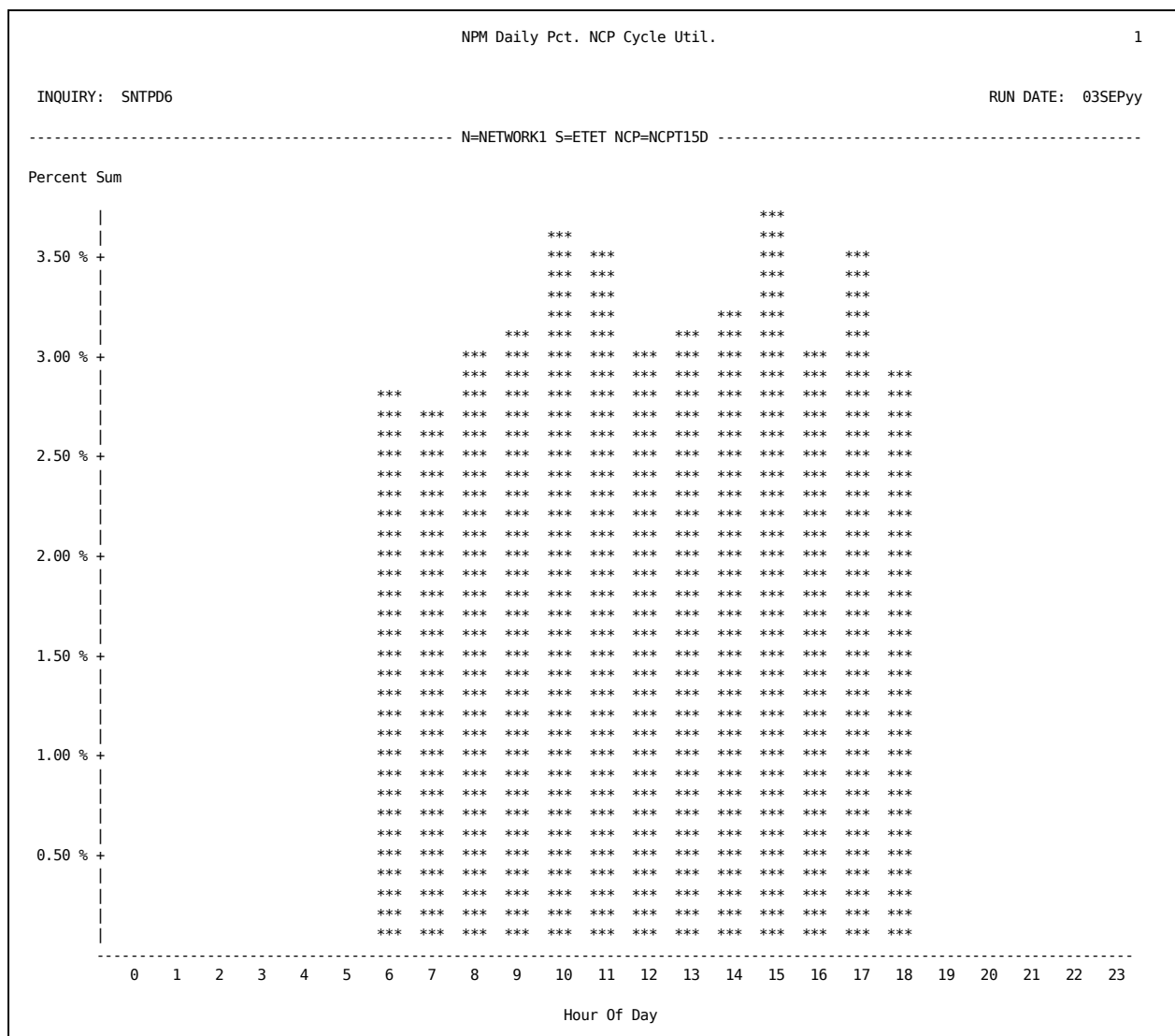


Figure 3-

3.3.1.3.2 NPM Daily NCP Buffer Utilization

INTENDED USE:

This chart helps determine the adequacy and utilization of memory in the communications control unit (CCU).

FORMAT:

This display produces a vertical bar chart of average free buffer queue length in the network control program by hour.

INQUIRY ID:

Color Graphics: SNTCD7

Printer Graphics: SNTPD7

DATA SOURCE (File/Timespan):

SNTNAF01 - Previous day

DATA ELEMENTS USED:

HOURL, NAFVFBQ, NCPNAME

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This inquiry is produced from Network Performance Monitor (NPM) network data. After the NCP load module (NCPGEN) is loaded into the CCU, the remaining memory is allocated for buffers. Thus, the buffering capacity of the CCU is a function of the size of the NCPGEN and the amount of installed memory in the CCU. The maximum available NCP buffer's value is the number of buffers initially allocated. The average free buffer queue length indicates the number of buffers that are generally available. The free buffer low-water mark is the lowest number of buffers that were available during the interval. The average free buffer count at slowdown is the number of buffers that were left when the CCU became severely memory-constrained.

Network performance is being impaired if the free buffer low-water mark is consistently below the average free buffer count at slowdown. A memory upgrade (if possible) should be considered if the average free buffer queue length is consistently close to the average free buffer count at slowdown. Otherwise, some of the load on the CCU may have to be shifted to another unit.

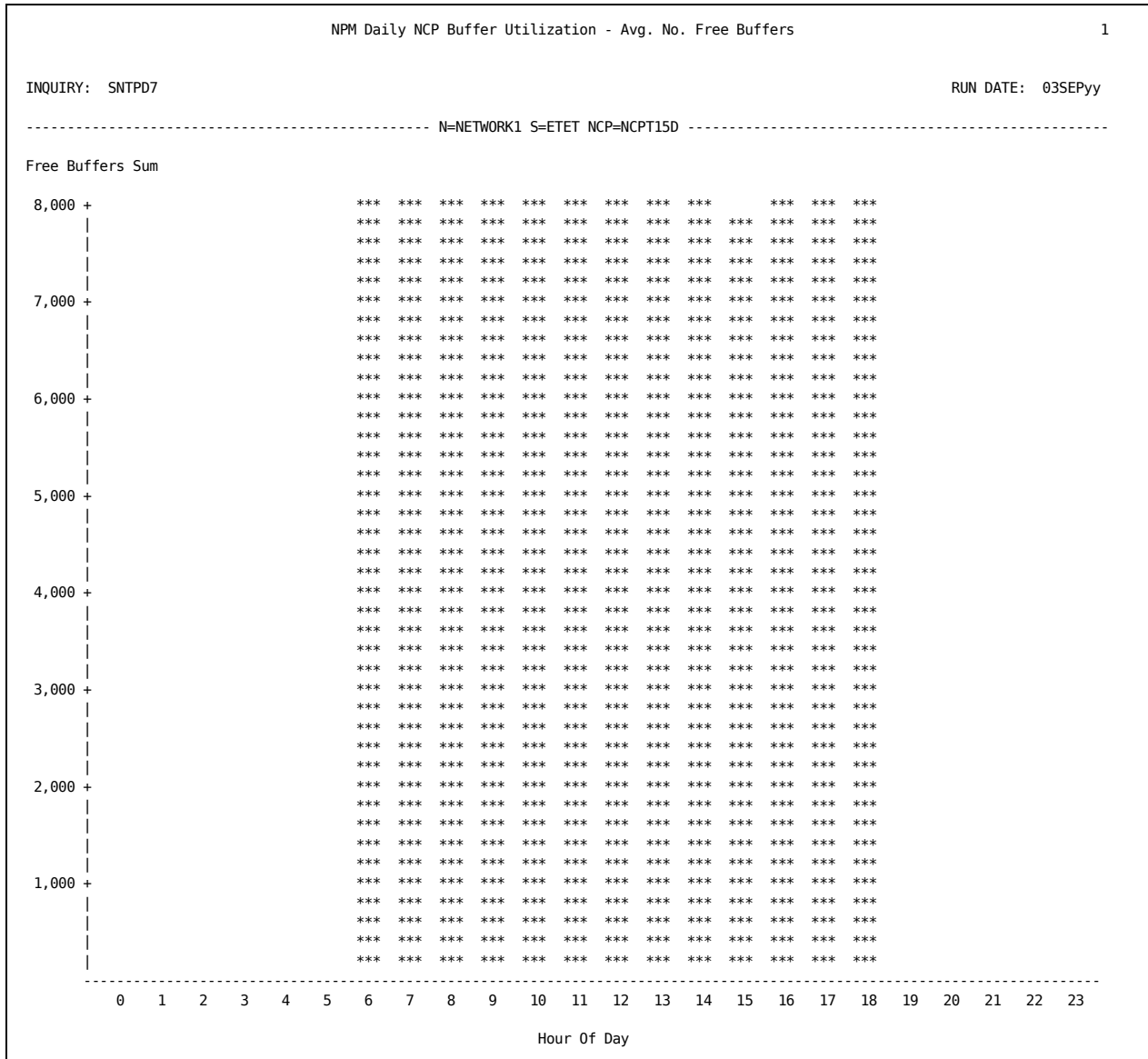


Figure 3-

3.3.1.3.3 NPM Daily Link Utilization

INTENDED USE:

This chart is used to determine the traffic fluctuation on a link over a period of 24 hours. This helps determine the need for changes to the configuration, such as the addition of links or an increase in the link speed.

FORMAT:

This display produces a vertical bar chart of the percentage link utilization by hour for an individual link.

INQUIRY ID:

Color Graphics: SNTCD8

Printer Graphics: N/A

DATA SOURCE (File/Timespan):

SNTNCL01 - Previous day

DATA ELEMENTS USED:

HOURL, NETNAME, NCLPCLBS

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This inquiry is produced from NetView Performance Monitor (NPM) network data. Percent Link Utilization is based on the specification of Link Speed in an NCP parameter. If the actual speed of the link differs from the speed specified for the NCP, the percentage displayed on this inquiry will be in error.

3.3.1.3.4 NetSpy Daily Pct. NCP Cycle Utilization

INTENDED USE:

This chart is used to determine the communications processor load variation (communications controller utilization cycles) over a period of 24 hours.

FORMAT:

This display produces a vertical bar chart of communications controller processor percentage utilization by hour.

INQUIRY ID:

Color Graphics: SNTCDP
Printer Graphics: SNTDPDP

DATA SOURCE (File/Timespan):

SNTNAF01 - Previous day

DATA ELEMENTS USED:

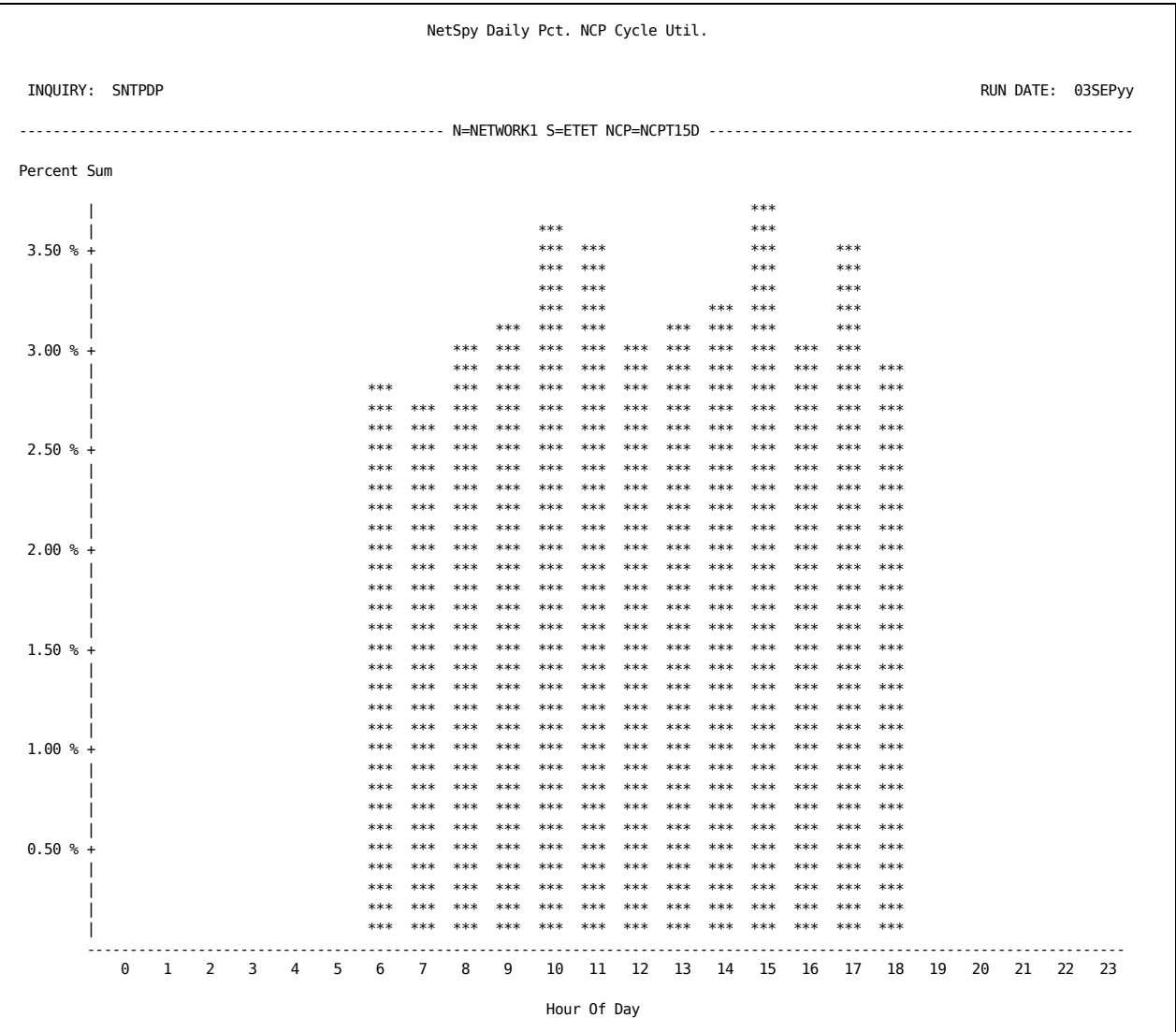
HOUR, NAFPCCU, NCPNAME

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This inquiry is produced from the CA NetSpy NCP interface data.



3.3.1.3.5 NetSpy Daily NCP Buffer Utilization

INTENDED USE:

This chart helps determine the adequacy and utilization of memory in the communications control unit (CCU).

FORMAT:

This display produces a vertical bar chart of average free buffer queue length in the network control program by hour.

INQUIRY ID:

Color Graphics: SNTCDQ
Printer Graphics: SNTPDQ

DATA SOURCE (File/Timespan):

SNTNAF01 - Previous day

DATA ELEMENTS USED:

HOUR, NAFVFBQ, NCPNAME

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This inquiry is produced from the CA NetSpy NCP interface data. After the NCP load module (NCPGEN) is loaded into the CCU, the remaining memory is allocated for buffers. Thus, the buffering capacity of the CCU is a function of the size of the NCPGEN and the amount of installed memory in the CCU. The maximum available NCP buffer's value is the number of buffers initially allocated. The average free buffer queue length indicates the number of buffers that are generally available. The free buffer low-water mark is the lowest number of buffers that were available during the interval. The average free buffer count at slowdown is the number of buffers that were left when the CCU became severely memory-constrained.

Network performance is being impaired if the free buffer low-water mark is consistently below the average free buffer count at slowdown. A memory upgrade (if possible) should be considered if the average free buffer queue length is consistently close to the average free buffer count at slowdown. Otherwise, some of the load on the CCU may have to be shifted to another unit.

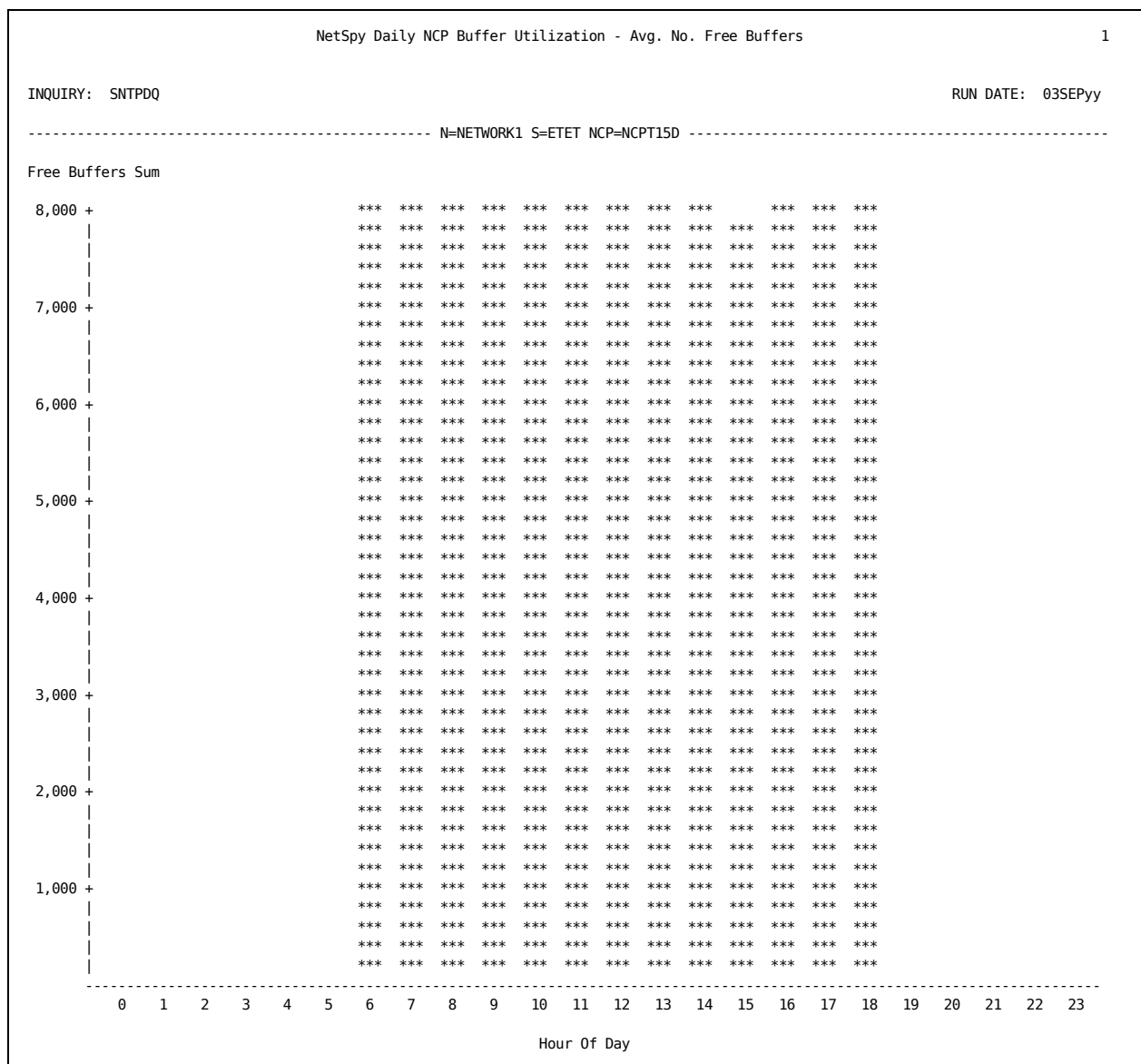


Figure 3-

3.3.1.3.6 NetSpy Daily Link Utilization

INTENDED USE:

This chart is used to determine the traffic fluctuation on a link over a period of 24 hours. This helps determine the need for changes to the configuration, such as the addition of links or an increase in the link speed.

FORMAT:

This display produces a vertical bar chart of the percentage link utilization by hour for an individual link.

INQUIRY ID:

Color Graphics: SNTCDR

Printer Graphics: N/A

DATA SOURCE (File/Timespan):

SNTNCL01 - Previous day

DATA ELEMENTS USED:

HOURL, NETNAME, NCLPCLBS

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This inquiry is produced from the CA NetSpy NCP interface data. Percent Link Utilization is based on the specification of Link Speed in an NCP parameter. If the actual speed of the link differs from the speed specified for the NCP, the percentage displayed on this inquiry will be in error.

3.3.1.3.7 NCP Utilization Ranking

INTENDED USE:

To rank all or selected NCPs in ascending or descending order based on CCU utilization or buffer utilization. The user chooses the number of NCPs ranked; the order of ranking; the variable used to rank on; and in the case of the SNTLXE and SNTLXF inquiries, the CCU and buffer thresholds. The report provides both CCU and buffer utilization information that can be used to identify NCPs having high utilization and possible overload conditions.

FORMAT:

A 9 column report (for SNTLDE a SNTLDF) or a 13 column report (for SNTLXE and SNTLXF) that is approximately 132 characters wide. It is best suited for hardcopy review but can be reviewed online. The information is summarized and presented by NETWRKID, SYSID, NCPNAME, Data Range, and Zone or Zone by Hour.

INQUIRY ID:

SNTLDE - NCPs w/in zone - DAYS timespan
SNTLDF - NCPs w/in hour - DAYS timespan
SNTLXE - NCPs w/in zone - DETAIL timespan
SNTLXF - NCPs w/in hour - DETAIL timespan

DATA SOURCE (File/Timespan):

SNTNAF - Days (SNTLDE, SNTLDF)
SNTNAF - Detail (SNTLXE, SNTLXF)

DATA ELEMENTS USED:

SNTLXE/SNTLXF

DURATION, NCPNAME, NAFPCCCU, NAFMXCCU, NAFMNCCU, NAFOVLM, NAFUNLIM, NAFPCNBU, NAFMXNBU, NAFMNNBU, NAFOVBLM, RANKLBL, NAFUNBLM, NAFPTIS, NETWRKID, SYSID, DATA, ZONE, DATE, TIME, CURRENT, IQ, HICCUDUR, HIBUFDUR, LOCCUDUR, LOBUFDUR

SNTLDE/SNTLDF

DURATION, NCPNAME, NAFPCCCU, NAFMXCCU, NAFMNCCU, NAFPCNBU, NAFMXNBU, NAFMNNBU, NAFPTIS, NETWRKID, SYSID, DATA, ZONE, RANKELEM, RANKLBL, CURRENT, IQ

CALCULATIONS:

```

SNTLXE/SNTLXF

/* Data Element Derivation (DATE) */;
FORMAT DATE DATE7.;
LABEL DATE="Date Selection Field";
DATE = DATEPART(ENDTS);
;
/* Data Element Derivation (TIME) */;
FORMAT TIME TIME11.2;
LABEL TIME="Time Selection Field";
TIME = TIMEPART(ENDTS);
;
/* Data Element Derivation (DATA) */;
LENGTH DATA $15;
FORMAT DATA $CHAR15.;
LABEL DATA="DATA RANGE";
DATA = ' ';
RETAIN DATEA DATEB;
LENGTH DATEA DATEB 4.;
DATEA = MIN(DATEA,STARTTS);
DATEB=MAX(DATEB,ENDTS);
IF _EOF_ THEN DO;
    DATEA=DATEPART(DATEA);
    DATEB=DATEPART(DATEB);
    SUBSTR(DATA,1,7)=PUT(DATEA,DATE7.);
    SUBSTR(DATA,8,1)='- ';
    SUBSTR(DATA,9,7)=PUT(DATEB,DATE7.);
    CALL SYMPUT('S',DATA);
    %GLOBAL S;
    DROP DATEA DATEB;
END;
/* Data Summarization */
%MACRO NEGATE;
    DATA=SYMGET('S');
%MEND NEGATE;
;
/* Data Element Derivation (HICCUDUR) */;
FORMAT HICCUDUR 8.;
LABEL HICCUDUR="TIME OVER CCU MAX LIMIT";
HICCUDUR = 0;
HV=SYMGET('HICCU');
HV=COMPRESS(HV,'% ');
HVCD=INPUT(HV,4.);
IF NAFPCCU GT HVCD THEN HICCUDUR=DURATION;
;
/* Data Element Derivation (HIBUFDUR) */;
FORMAT HIBUFDUR 8.;

```

```

LABEL HIBUFDUR="TIME OVER CCU BUFFER MAX LIMIT";
HIBUFDUR = 0;
HV=SYMGET('HIBUFF');
HV=COMPRESS(HV,'% ');
HVBD=INPUT(HV,4.);
IF NAFPCNBU GT HVBD THEN HIBUFDUR=DURATION;
;
/* Data Element Derivation (LOCCUDUR) */;
FORMAT LOCCUDUR 8.;
LABEL LOCCUDUR="TIME UNDER CCU MIN LIMIT";
LOCCUDUR = 0;
LV=SYMGET('LOWCCU');
LV=COMPRESS(LV,'% ');
LVCD=INPUT(LV,4.);
IF NAFPCCCU LT LVCD THEN LOCCUDUR=DURATION;
;
/* Data Element Derivation (LOBUFDUR) */;
FORMAT LOBUFDUR 8.;
LABEL LOBUFDUR="TIME UNDER CCU BUFFER MIN LIMIT";
LOBUFDUR = 0;
LV=SYMGET('LOWBUFF');
LV=COMPRESS(LV,'% ');
LVBD=INPUT(LV,4.);
IF NAFPCNBU LT LVBD THEN LOBUFDUR=DURATION;
;
/* Data Element Derivation (CURRENT, &C) */;
FORMAT CURRENT WEEKDATE15.;
LABEL CURRENT="CURRENT DATE";
CURRENT = TODAY();
C=PUT(CURRENT,WEEKDATE15.);
C=COMPRESS(C);
CALL SYMPUT('C',PUT(C,$CHAR12.));
%GLOBAL C;
;
/* Data Element Derivation (IQ, &I) */;
LENGTH IQ $8;
FORMAT IQ $CHAR8.;
LABEL IQ="Inquire Name";
IQ = ' ';
SUBSTR(IQ,1,1)='(';
SUBSTR(IQ,2,6)=SYMGET('INQINAME');
SUBSTR(IQ,8,1)=')';
CALL SYMPUT('I',PUT(IQ,$CHAR8.));
%GLOBAL I;
;
/* Data Element Derivation (RANKELEM) */;
FORMAT RANKELEM 8.;
LABEL RANKELEM="&RL";
RANKELEM = &RANKELEM;
```



```

;
/* Data Element Derivation (RANKLBL) */;
LENGTH RANKLBL $40;
FORMAT RANKLBL $CHAR40.;
LABEL RANKLBL="LABEL OF RANKING ELEMENT";
RANKLBL = SYMGET('RL');
;
/* Data Element Derivation (NAFOVLIM) */;
FORMAT NAFOVLIM MAPCT8.;
LABEL NAFOVLIM="% TIME CCU UTILIZATION ABOVE THRESHOLD";
NAFOVLIM = 0;
IF DURATION GT 0 THEN NAFOVLIM=(HICCUDUR/DURATION)*100;
;
/* Data Element Derivation (NAFUNLIM) */;
FORMAT NAFUNLIM MAPCT8.;
LABEL NAFUNLIM="% TIME CCU UTILIZATION BELOW THRESHOLD";
NAFUNLIM = 0;
IF DURATION GT 0 THEN NAFUNLIM=(LOCCUDUR/DURATION)*100;
;
/* Data Element Derivation (NAFOVBLM) */;
FORMAT NAFOVBLM MAPCT8.;
LABEL NAFOVBLM="% TIME CCU BUFFER UTLZ OVER THRESHOLD";
NAFOVBLM = 0;
IF DURATION GT 0 THEN NAFOVBLM=(HIBUFDUR/DURATION)*100;
;
/* Data Element Derivation (NAFUNBLM) */;
FORMAT NAFUNBLM MAPCT8.;
LABEL NAFUNBLM="% TIME CCU BUFFER UTLZ BELOW THRESHOLD";
NAFUNBLM = 0;
IF DURATION GT 0 THEN NAFUNBLM=(LOBUFDUR/DURATION)*100;
;

SNTLDE/SNTLDF

/* Data Element Derivation (DATE) */;
FORMAT DATE DATE7.;
LABEL DATE="Date Selection Field";
DATE = DATEPART(ENDTS);
;
/* Data Element Derivation (TIME) */;
FORMAT TIME TIME11.2;
LABEL TIME="Time Selection Field";
TIME = TIMEPART(ENDTS);
;
/* Data Element Derivation (DATA) */;
LENGTH DATA $15;
FORMAT DATA $CHAR15.;
LABEL DATA="DATA RANGE";

```

```
DATA = ' ';
/* SAS System Statements(Derive vars & data select) */;
RETAIN DATEA DATEB;
LENGTH DATEA DATEB 4.;
DATEA = MIN(DATEA,STARTTS);
DATEB=MAX(DATEB,ENDTS);
IF _EOF_ THEN DO;
    DATEA=DATEPART(DATEA);
    DATEB=DATEPART(DATEB);
    SUBSTR(DATA,1,7)=PUT(DATEA,DATE7.);
    SUBSTR(DATA,8,1)='- ';
    SUBSTR(DATA,9,7)=PUT(DATEB,DATE7.);
    CALL SYMPUT('S',DATA);
    %GLOBAL S;
    DROP DATEA DATEB;
END;
/* Data Summarization */
%MACRO NEGATE;
    DATA=SYMGET('S');
%MEND NEGATE;
;
/* Data Element Derivation (CURRENT, &C) */;
FORMAT CURRENT WEEKDATE15.;
LABEL CURRENT="CURRENT DATE";
CURRENT = TODAY();
C=PUT(CURRENT,WEEKDATE15.);
C=COMPRESS(C);
CALL SYMPUT('C',PUT(C,$CHAR12.));
%GLOBAL C;
;
/* Data Element Derivation (IQ, &I) */;
LENGTH IQ $8;
FORMAT IQ $CHAR8.;
LABEL IQ="Inquire Name";
IQ = ' ';
SUBSTR(IQ,1,1)='(';
SUBSTR(IQ,2,6)=SYMGET('INQINAME');
SUBSTR(IQ,8,1)=')';
CALL SYMPUT('I',PUT(IQ,$CHAR8.));
%GLOBAL I;
;
/* Data Element Derivation (RANKELEM) */;
FORMAT RANKELEM 8.;
LABEL RANKELEM="&RL";
RANKELEM = &RANKELEM;
;
/* Data Element Derivation (RANKLBL) */;
LENGTH RANKLBL $40;
FORMAT RANKLBL $CHAR40.;
```

```
LABEL RANKLBL="LABEL OF RANKING ELEMENT";
RANKLBL = SYMGET('RL');
;
```

USAGE CONSIDERATIONS:

All cycles are summarized together as a data range rather than reporting by individual cycle or by year, month, day, and hour as other CA MICS reports do.

1

(SNTLDE) DAILY NCP UTILIZATION RANKING BY ZONE									
FIRST 10 NCPS BY DESCENDING PERCENT COMMUNICATIONS CONTROLLER UTIL.									
NETWORK ID: NETWORK1 SYSTEM ID: SYS1 DATA RANGE: 040CTyy-17JUNyy ZONE: 1									
----- IDENTIFICATION ----- ----- UTILIZATION INFORMATION -----									
DURATION(HH:MM) / ----- CCU ----- ----- BUFFERS ----- TIME IN									
NCP NAME AVG MAX MIN AVG MAX MIN SLOWDOWN									
=====									
1:00	PEP12E	55.74 %	56.05 %	55.29 %	1.67 %	11.22 %	0.12 %	0.00 %	
1:00	GWN2AM	43.72 %	46.49 %	39.76 %	7.26 %	34.05 %	0.43 %	0.00 %	
=====									
DATES=NONE, TIME=(00:00-24:00), RANKING=NAFPCCCU=PERCENT COMMUNICATIONS CONTROLLER UTIL.									
RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NAF									

2

```

(SNTLDE) DAILY NCP UTILIZATION RANKING BY ZONE
FIRST 10 NCPS BY DESCENDING PERCENT COMMUNICATIONS CONTROLLER UTIL.
NETWORK ID: NETWORK1 SYSTEM ID: SYS2 DATA RANGE: 040CTyy-17JUNyy ZONE: 1
|-IDENTIFICATION--||-----UTILIZATION INFORMATION-----|
|DURATION(HH:MM) /||-----CCU-----|-----BUFFERS-----| TIME IN |
| NCP NAME || AVG MAX MIN | AVG MAX MIN | SLOWDOWN |
=====
9:05 NCPT15D 3.24 % 5.07 % 2.69 % 4.85 % 23.77 % 4.31 % 0.00 %

```

DATES=NONE, TIME=(00:00-24:00), RANKING=NAFPCCCU=PERCENT COMMUNICATIONS CONTROLLER UTIL.
 RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NAF

3

```

(SNTLDE) DAILY NCP UTILIZATION RANKING BY ZONE
FIRST 10 NCPS BY DESCENDING PERCENT COMMUNICATIONS CONTROLLER UTIL.
NETWORK ID: NETWORK1 SYSTEM ID: SYS3 DATA RANGE: 040CTyy-17JUNyy ZONE: 2
|-IDENTIFICATION--||-----UTILIZATION INFORMATION-----|
|DURATION(HH:MM) /||-----CCU-----|-----BUFFERS-----| TIME IN |
| NCP NAME || AVG MAX MIN | AVG MAX MIN | SLOWDOWN |
=====
3:28 NCPT15D 2.97 % 4.59 % 2.61 % 4.79 % 23.41 % 4.31 % 0.00 %

```

DATES=NONE, TIME=(00:00-24:00), RANKING=NAFPCCCU=PERCENT COMMUNICATIONS CONTROLLER UTIL.
 RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NAF

4

```

(SNTLDE) DAILY NCP UTILIZATION RANKING BY ZONE
FIRST 10 NCPS BY DESCENDING PERCENT COMMUNICATIONS CONTROLLER UTIL.
NETWORK ID: NETWORK1 SYSTEM ID: SYS4 DATA RANGE: 040CTyy-17JUNyy ZONE: 2
|-IDENTIFICATION--|-----UTILIZATION INFORMATION-----|
|DURATION(HH:MM) /|-----CCU-----|-----BUFFERS-----|TIME IN|
|NCP NAME||AVG|MAX|MIN|AVG|MAX|MIN|SLOWDOWN|
=====
0:15 IPCNCPG 32.69 % 32.69 % 32.69 % 6.11 % 8.45 % 3.94 % 0.00 %
0:15 IPCNCPH 32.24 % 32.24 % 32.24 % 3.11 % 5.01 % 2.21 % 0.00 %
0:15 TYONCPA 25.50 % 25.50 % 25.50 % 0.83 % 1.88 % 0.49 % 0.00 %
0:15 BRNNCPF 23.33 % 23.33 % 23.33 % 3.75 % 11.63 % 3.56 % 0.00 %
0:15 BRNNCPD 23.13 % 23.13 % 23.13 % 15.27 % 21.72 % 14.23 % 0.00 %
0:15 IPCNCPK 22.78 % 22.78 % 22.78 % 2.97 % 3.38 % 2.41 % 0.00 %
0:15 SINNCPE 19.89 % 19.89 % 19.89 % 8.52 % 11.59 % 6.98 % 0.00 %
0:15 IPCNCPD 19.70 % 19.70 % 19.70 % 4.18 % 5.21 % 2.92 % 0.00 %
0:15 BKKNCPE 17.45 % 17.45 % 17.45 % 1.04 % 1.80 % 0.95 % 0.00 %
0:15 IPCNCPF 16.68 % 16.68 % 16.68 % 3.64 % 5.83 % 3.05 % 0.00 %

```

DATES=NONE, TIME=(00:00-24:00), RANKING=NAFPCCCU=PERCENT COMMUNICATIONS CONTROLLER UTIL.
 RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NAF

5

```

(SNTLDE) DAILY NCP UTILIZATION RANKING BY ZONE
FIRST 10 NCPS BY DESCENDING PERCENT COMMUNICATIONS CONTROLLER UTIL.
NETWORK ID: NETWORK1 SYSTEM ID: SYS5 DATA RANGE: 040CTyy-17JUNyy ZONE: 1
|-IDENTIFICATION--|-----UTILIZATION INFORMATION-----|
|DURATION(HH:MM) /|-----CCU-----|-----BUFFERS-----|TIME IN|
|NCP NAME||AVG|MAX|MIN|AVG|MAX|MIN|SLOWDOWN|
=====
0:06 N13G5C0 3.90 % 4.94 % 3.51 % 4.27 % 12.31 % 0.89 % 0.00 %

```

DATES=NONE, TIME=(00:00-24:00), RANKING=NAFPCCCU=PERCENT COMMUNICATIONS CONTROLLER UTIL.
 RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NAF

6

(SNTLDE) DAILY NCP UTILIZATION RANKING BY ZONE
FIRST 10 NCPS BY DESCENDING PERCENT COMMUNICATIONS CONTROLLER UTIL.
NETWORK ID: NETWORK1 SYSTEM ID: SYS6 DATA RANGE: 040CTyy-17JUNyy ZONE: 2

IDENTIFICATION		UTILIZATION INFORMATION						
DURATION(HH:MM)		CCU			BUFFERS			TIME IN
NCP NAME		AVG	MAX	MIN	AVG	MAX	MIN	SLOWDOWN
0:28	A30N2	5.41 %	5.52 %	5.34 %	12.50 %	17.65 %	7.04 %	0.00 %
0:28	A40N2	2.88 %	2.94 %	2.80 %	1.13 %	1.84 %	1.00 %	0.00 %

DATES=NONE, TIME=(00:00-24:00), RANKING=NAFPCCU=PERCENT COMMUNICATIONS CONTROLLER UTIL.
RUN-DATE=Wed,Sep3,yy , TIMESPAN=DAYS, DBID=8, FILE=NAF

Figure 3-

3.3.1.3.8 NCP Utilization Chart

INTENDED USE:

This chart indicates the NCP, buffer, and slowdown percentages presented side by side for each hour within a zone. A user-specified maximum CCU utilization reference line is drawn on the chart to indicate the objective response time for the NCP.

FORMAT:

This display produces a horizontal bar chart showing average CCU, buffer, and slowdown percentages by hour within a zone. It can be used to identify periods of time when utilization exceeded the established user maximum. The data is summarized and presented by NETWRKID, SYSID, NCPNAME, Year, Month, Day, and Zone by Hour.

INQUIRY ID:

SNTPDU

DATA SOURCE (File/Timespan):

SNTNAF - Days

DATA ELEMENTS USED:

NAFPCCCU, NAFPCTIS, NAFPCNBU, DATE, TIME, CURRENT, IQ, PERCENT, NETWRKID, SYSID, NCPNAME, YEAR, MONTH, DAY, ZONE, HOUR

CALCULATIONS:

```
/* Data Element Derivation (DATE) */;
FORMAT DATE DATE7.;
LABEL DATE="Date Selection Field";
DATE = DATEPART(ENDTS);
;
/* Data Element Derivation (TIME) */;
FORMAT TIME TIME11.2;
LABEL TIME="Time Selection Field";
TIME = TIMEPART(ENDTS);
;
/* Data Element Derivation (CURRENT, &C) */;
FORMAT CURRENT WEEKDATE15.;
LABEL CURRENT="CURRENT DATE";
CURRENT = TODAY();
```

```
C=PUT(CURRENT,WEEKDATE15.);
C=COMPRESS(C) ;
CALL SYMPUT('C',PUT(C,$CHAR12.));
%GLOBAL C;
;
/* Data Element Derivation (IQ, &I) */;
LENGTH IQ $8;
FORMAT IQ $CHAR8.;
LABEL IQ="Inquire Name";
IQ = ' ';
SUBSTR(IQ,1,1)='(';
SUBSTR(IQ,2,6)=SYMGET('INQINAME');
SUBSTR(IQ,8,1)=')';
CALL SYMPUT('I',PUT(IQ,$CHAR8.));
%GLOBAL I;
;
/* Data Element Derivation (PERCENT) */;
FORMAT PERCENT 8.;
LABEL PERCENT="PERCENT UTILIZATION";
PERCENT = .;
;
/* Data Element Derivation (Create & Load NAME,
  & Load PERCENT) */;
LENGTH NAME $1;
FORMAT NAME $1.;
LABEL NAME="VARIABLE TO PLOT";
NAME = 'C'; PERCENT=NAFPCCCU;
OUTPUT;
NAME = 'S'; PERCENT=NAFPCTIS;
OUTPUT;
NAME = 'B'; PERCENT=NAFPCNBU;
OUTPUT;
IF PERCENT=. THEN PERCENT=0;
;
```

USAGE CONSIDERATIONS:

None

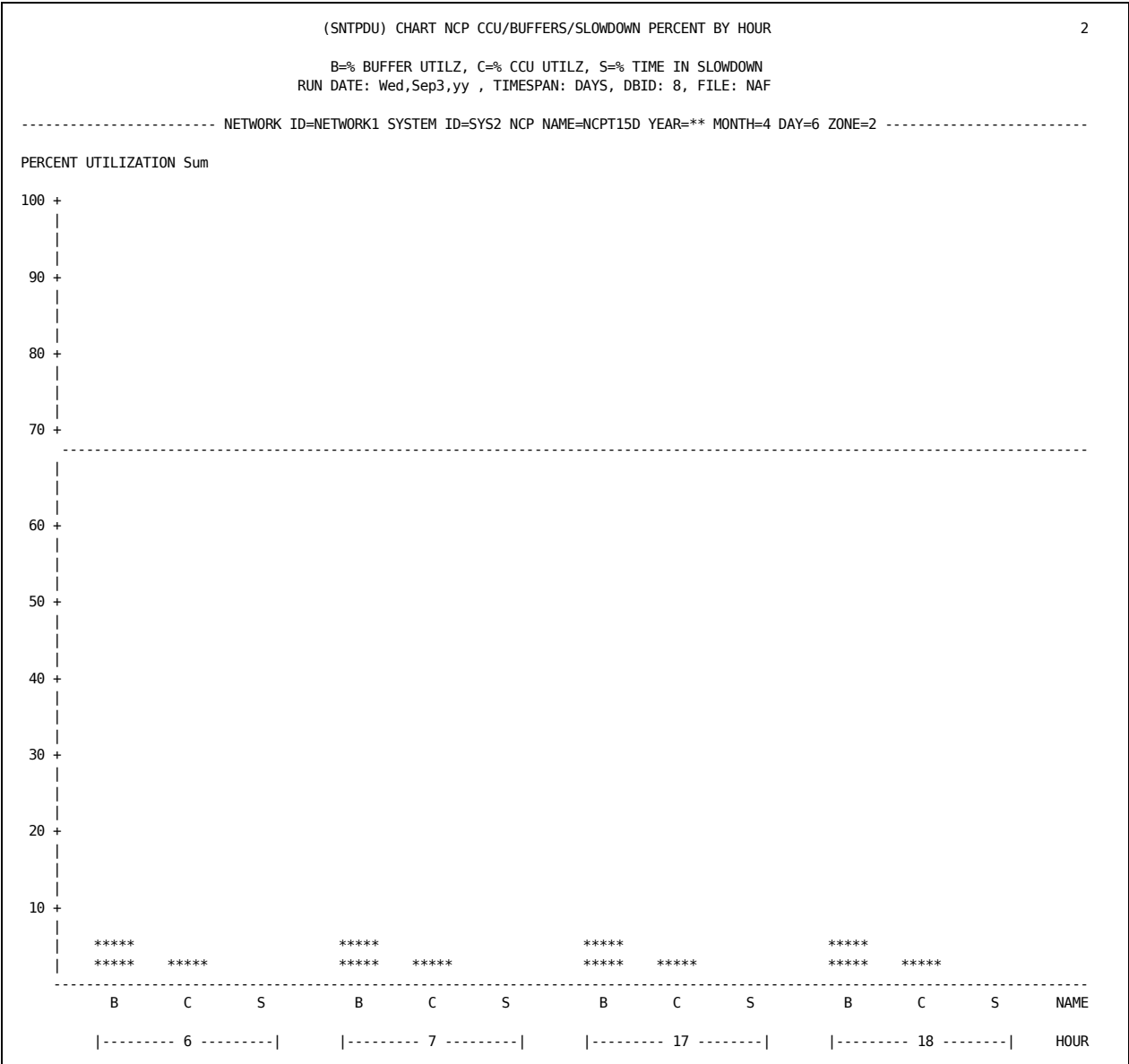


Figure 3-

3.3.1.3.9 NCP Utilization Plot

INTENDED USE:

This plot indicates the NCP, buffer, and slowdown percentages for each hour of the day. A user-specified maximum CCU utilization reference line is drawn on the chart to indicate the objective response time for the NCP. Zone reference lines are also drawn on the plot and can be modified to match those zones established at the site.

FORMAT:

This display produces a overlay plot showing average CCU, buffer, and slowdown percentages by hour of day for 24 hours. It can be used to identify periods of time when utilization exceeded the established user maximum. The data is summarized and presented by NETWRKID, SYSID, NCPNAME, Year, Month, and Day, by Hour.

INQUIRY ID:

SNTPDV

DATA SOURCE (File/Timespan):

SNTNAF - Days

DATA ELEMENTS USED:

NAFPCCCU, NAFPCTIS, NAFPNCBU, DATE, TIME, CURRENT, IQ, PERCENT, NETWRKID, SYSID, NCPNAME, YEAR, MONTH, DAY, HOUR

CALCULATIONS:

```
/* Data Element Derivation (DATE) */;
FORMAT DATE DATE7.;
LABEL DATE="Date Selection Field";
DATE = DATEPART(ENDTS);
;
/* Data Element Derivation (TIME) */;
FORMAT TIME TIME11.2;
LABEL TIME="Time Selection Field";
TIME = TIMEPART(ENDTS);
;
/* Data Element Derivation (CURRENT, &C) */;
FORMAT CURRENT WEEKDATE15.;
LABEL CURRENT="CURRENT DATE";
```

```
CURRENT = TODAY();
C=PUT(CURRENT,WEEKDATE15.);
C=COMPRESS(C) ;
CALL SYMPUT('C',PUT(C,$CHAR12.));
%GLOBAL C;
;
/* Data Element Derivation (IQ, &I) */;
LENGTH IQ $8;
FORMAT IQ $CHAR8.;
LABEL IQ="Inquire Name";
IQ = ' ';
SUBSTR(IQ,1,1)='(';
SUBSTR(IQ,2,6)=SYMGET('INQINAME');
SUBSTR(IQ,8,1)=')';
CALL SYMPUT('I',PUT(IQ,$CHAR8.));
%GLOBAL I;
;
/* Data Element Derivation (PERCENT) */;
FORMAT PERCENT 8.;
LABEL PERCENT="PERCENT UTILIZATION";
PERCENT = .;
;
```

USAGE CONSIDERATIONS:

None

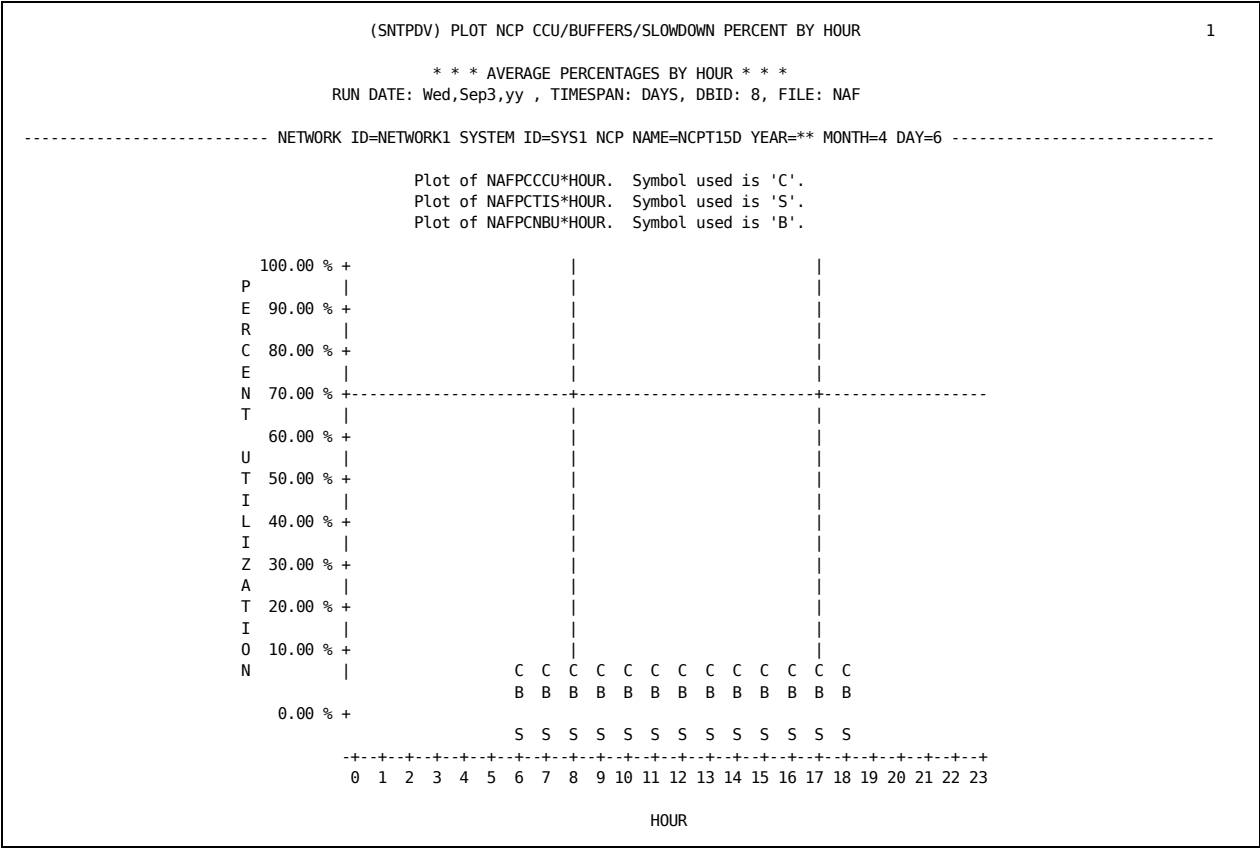


Figure 3-

3.3.1.3.10 NCP Channel Hold/Intermediate Queue Length Plot

INTENDED USE:

This plot indicates the queue lengths for NCP channel hold and intermediate queues for each hour of the day. A user-specified maximum NCP channel hold queue length reference line is drawn on the chart. Zone reference lines are also drawn on the plot and can be modified to match those zones established at the site.

FORMAT:

This display produces an overlay plot showing average and maximum NCP channel hold queue and intermediate queue lengths by hour of day for 24 hours. It can be used to identify periods of time when queue lengths have exceeded the established user maximum. The data is summarized and presented by NETWRKID, SYSID, NCPNAME, Year, Month, and Day, by Hour.

INQUIRY ID:

SNTPDW

DATA SOURCE (File/Timespan):

SNTNAF - Days

DATA ELEMENTS USED:

NAFAVHQL, NAFAVIQL, NAFMXHQL, NAFMXIQL, DATE, TIME, CURRENT, IQ, PERCENT, NETWRKID, SYSID, NCPNAME, YEAR, MONTH, DAY, HOUR

CALCULATIONS:

```
/* Data Element Derivation (DATE) */;
FORMAT DATE DATE7.;
LABEL DATE="Date Selection Field";
DATE = DATEPART(ENDTS);
;
/* Data Element Derivation (TIME) */;
FORMAT TIME TIME11.2;
LABEL TIME="Time Selection Field";
TIME = TIMEPART(ENDTS);
;
/* Data Element Derivation (CURRENT, &C) */;
FORMAT CURRENT WEEKDATE15.;
```

```

LABEL CURRENT="CURRENT DATE";
CURRENT = TODAY();
C=PUT(CURRENT,WEEKDATE15.);
C=COMPRESS(C) ;
CALL SYMPUT('C',PUT(C,$CHAR12.));
%GLOBAL C;
;
/* Data Element Derivation (IQ, &I) */;
LENGTH IQ $8;
FORMAT IQ $CHAR8.;
LABEL IQ="Inquire Name";
IQ = ' ';
SUBSTR(IQ,1,1)='(';
SUBSTR(IQ,2,6)=SYMGET('INQINAME');
SUBSTR(IQ,8,1)=')';
CALL SYMPUT('I',PUT(IQ,$CHAR8.));
%GLOBAL I;
;
/* Data Element Derivation (PERCENT) */;
FORMAT PERCENT 8.;
LABEL PERCENT="PERCENT UTILIZATION";
PERCENT = .;
;

```

USAGE CONSIDERATIONS:

None

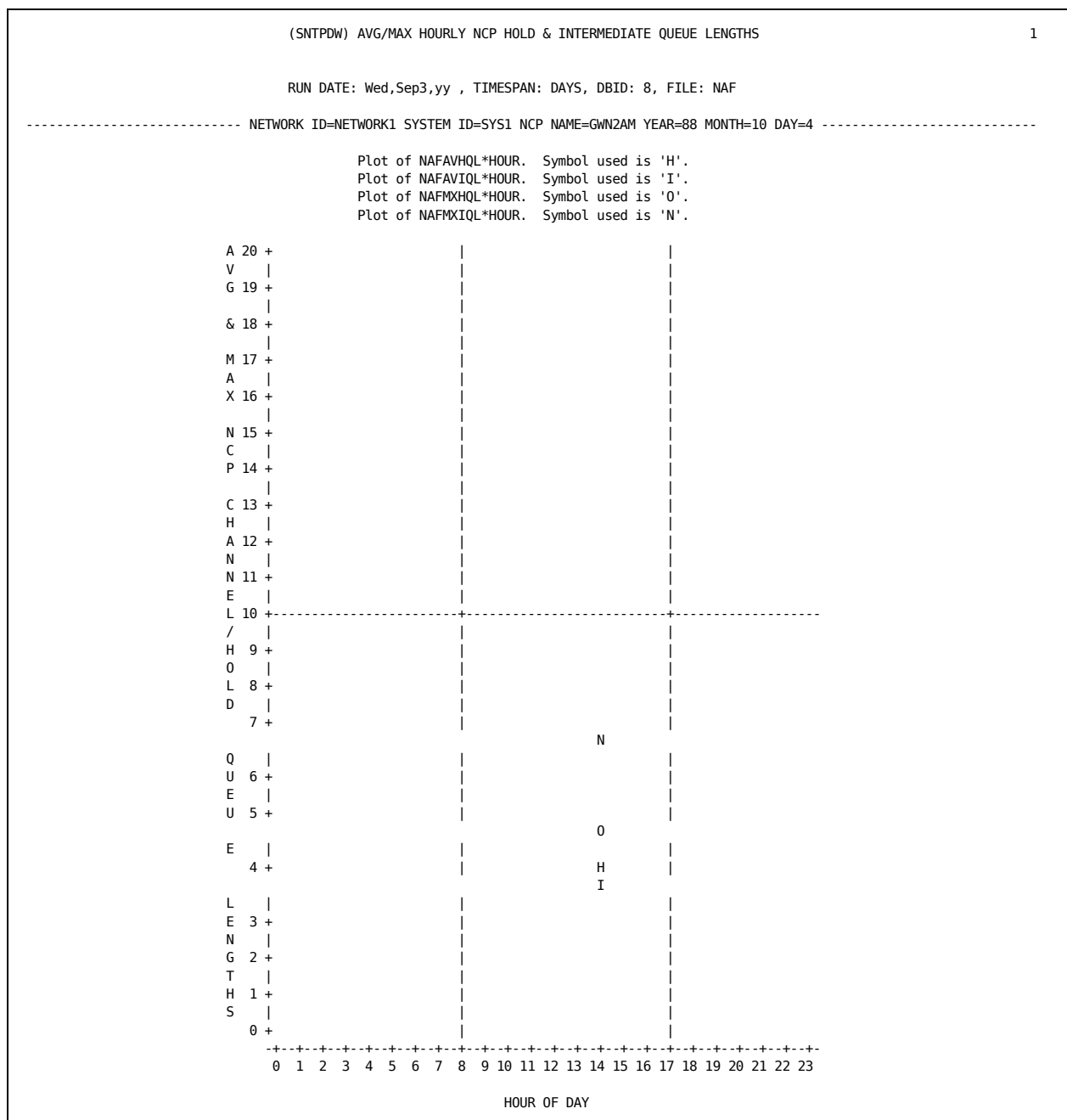


Figure 3-

3.3.1.3.11 NetSpy Daily Average VR Response Time

INTENDED USE:

This chart displays average virtual route response time. Virtual route response time is the time it takes for a message to traverse the logical route or backbone link between the primary logical unit subarea and the secondary logical unit subarea. The time required to traverse the virtual route extension (for example, the boundary link between an NCP and a cluster control unit) is excluded from virtual route response time. Compare virtual route response time measurements with total network response time measurements (for example, Average Network Response Time, NSSAVNTM) to determine if there is a bottleneck in either the virtual route or the virtual route extension.

FORMAT:

This display produces a vertical bar chart of average virtual route response time.

INQUIRY ID:

Color Graphics: SNTCD5
Printer Graphics: SNTPD5

DATA SOURCE (File/Timespan):

SNTNVR01 - Previous day

DATA ELEMENTS USED:

SYSID, NVRHSA, NVRDSA, NVRVRTE, NVRAVNTM, NVRNRSTM,
NVRNRESC

CALCULATIONS:

IF NVRNRESC GT ZERO THEN
 NVRAVNTM=NVRNRSTM / NVRNRESC;
ELSE NVRAVNTM=.;

USAGE CONSIDERATIONS:

Use in conjunction with SNTCDZ, CA NetSpy Daily Pct. Time VR Held/Blocked, to isolate virtual route performance problems. Also use with other MICF inquiries that measure link utilization and NCP buffer and cycle utilization to isolate the source of the congestion.

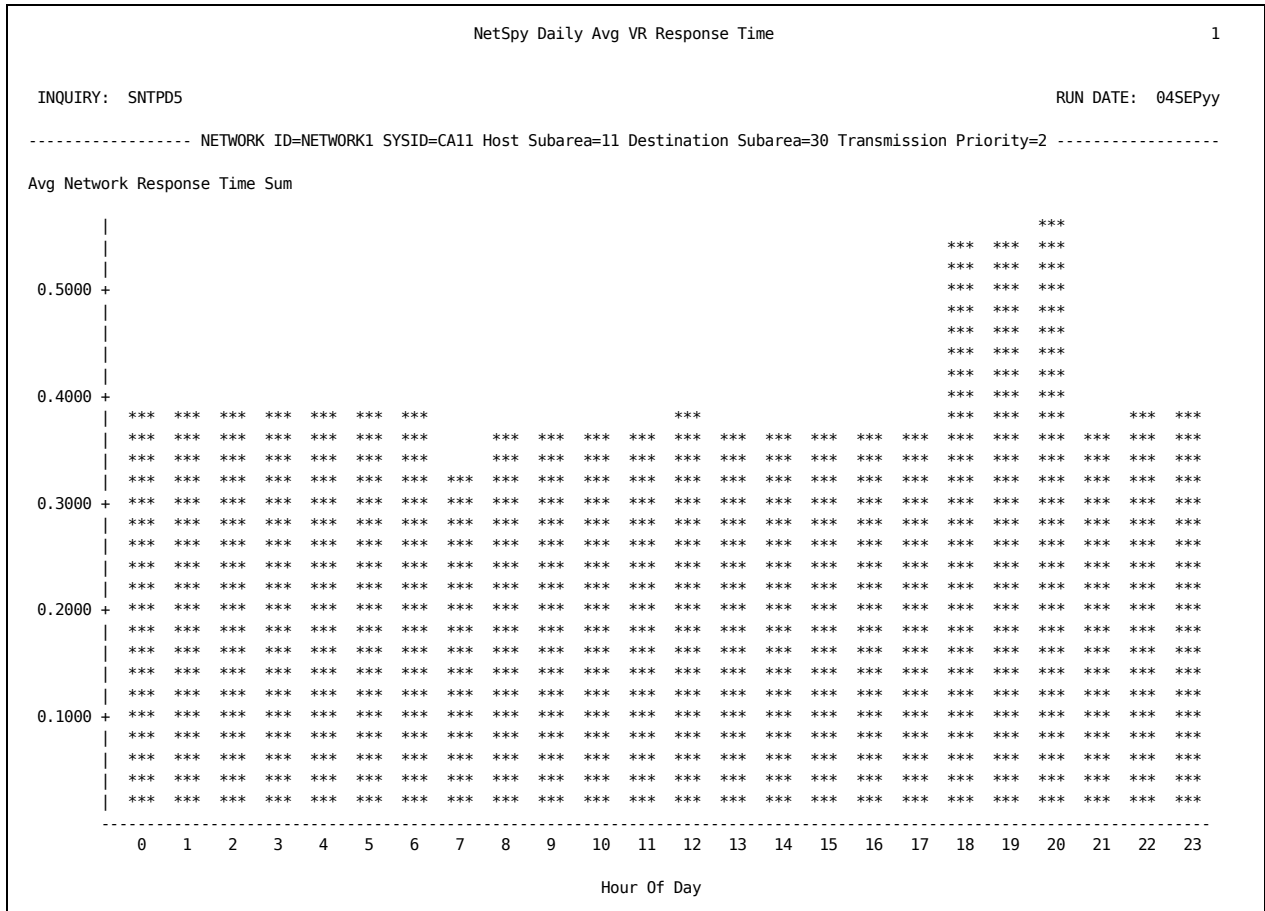


Figure 3-

3.3.1.3.12 NetSpy Daily % Time VR Held/Blocked

INTENDED USE:

This chart displays the percentage of time during the day that a virtual route (i.e., backbone link) is held or blocked. "Held" status is the first level of virtual route congestion; "Blocked" status is the highest level of congestion. End user response time is prolonged when a virtual route becomes held or blocked, because during that period no messages can be sent across the route. Virtual route congestion can be caused by such factors as insufficient buffers in a down stream NCP or an over-utilized boundary link.

FORMAT:

This display produces a vertical bar chart of the percentage of time that a virtual route is held or blocked.

INQUIRY ID:

Color Graphics: SNTCDZ
Printer Graphics: SNTPDZ

DATA SOURCE (File/Timespan):

SNTNVR01 - Previous day

DATA ELEMENTS USED:

SYSID, NVRHSA, NVRDSA, NVRVRTE, NVRPCTHL

CALCULATIONS:

None.

USAGE CONSIDERATIONS:

Use in conjunction with SNTCD5, NetSpy Daily Average VR Response Time, to isolate virtual route performance problems. Also use with other MICF inquiries that measure link utilization and NCP buffer and cycle utilization to isolate the source of the congestion.

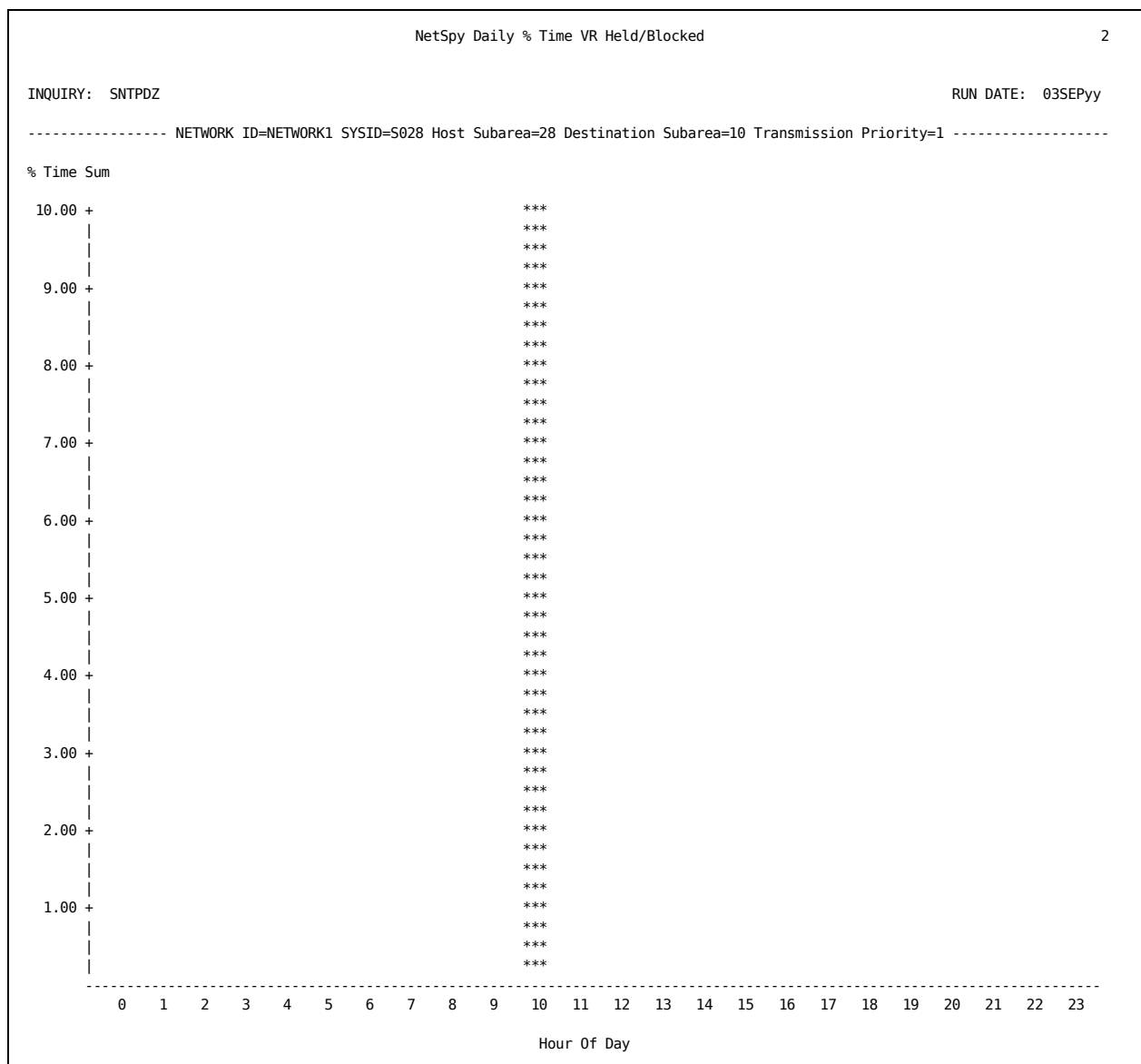


Figure 3-

3.3.1.3.13 Under/Over Utilized Line Analysis

INTENDED USE:

To identify, through a series of four reports, which lines in the network are underutilized, overutilized, or marginally-utilized, as determined by user-defined utilization thresholds. This inquiry indicates overutilized lines that may be causing performance problems and identifies underutilized lines whose resources might be combined with others to reduce the total number of lines in the network.

FORMAT:

Each report is approximately 132 characters wide and is best suited for hardcopy review. However, you can also review the reports online. The first report provides an overview of the count of network lines for each of the respective categories of under, marginally, and overutilized. The second report lists the underutilized lines in descending order, indicating line name, NCP name, hours underutilized, total hours measured, line speed, and data transfer mode (full or half duplex). The third report provides similar information for marginally-utilized lines. The fourth report lists the overutilized lines in descending order, showing line name, NCP name, hours overutilized, hours underutilized, and marginally-utilized, maximum percents received busy and send busy respectively, link speed, and data transfer mode. In reports two through four, the information is summarized and presented by NETWRKID and ranked (in descending order) by line utilization.

INQUIRY ID:

SNTLDS - Under/Over Utilized Line Analysis

DATA SOURCE (Files/Timespan):

SNTNCL - Days

DATA ELEMENTS USED:

ENDTS, STARTTS, NETNAME, NCPNAME, NCLMXRLB, NCLMXSLB,
NCLPCLBS, NCLNRLLS, NCLNRSLS, NETWRKID, ZONE

CALCULATIONS:

None

USAGE CONSIDERATIONS:

The user defines the thresholds (as run-time options) for overutilization, underutilization, and marginal utilization. This inquiry will never categorize a line as underutilized or marginally utilized if, during at least one measured interval, line utilization exceeds the client-defined threshold for overutilization.

All cycles are summarized together as a data range rather than reported by individual cycle or by year, month, day, and zone as other CA MICS reports do.

OVER/UNDER LINE UTILIZATION SUMMARY			1
INQUIRY: SNTLDS			RUN DATE: 03SEPyy
DATA RANGE - START: 06APR04:07:54		NETWORK: NETWORK1	
DATA RANGE - END: 06APR04:16:58		TIME ZONE: 1	
DESCRIPTION	COUNT	PERCENT	
NUMBER OF LINES UNDER UTILIZED	6	100.00 %	
NUMBER OF LINES marginally UTILIZED	0	0.00 %	
NUMBER OF LINES OVER UTILIZED	0	0.00 %	
TOTAL NUMBER OF LINES	6	100.00 %	
UNDER UTILIZED: LESS THAN OR EQUAL 7 PERCENT			
marginally UTILIZED: LESS THAN OR EQUAL 14 PERCENT			
OVER UTILIZED: GREATER THAN 60 PERCENT			

2

UNDER UTILIZED LINE REPORT

INQUIRY: SNTLDS

RUN DATE: 03SEPyy

DATA RANGE - START: 06APR04:07:54

NETWORK: NETWORK1

DATA RANGE - END: 06APR04:16:58

TIME ZONE: 1

Line Name	Datatype	NCP Name	Hours Under Utilized	Total Hours	Avg. Intvl Size	Send Line Speed
MCHLK97	X25	NCPT15D	9	9	0:08	64K
MCHLK95	X25	NCPT15D	9	9	0:08	64K
MCHLK80A	X25	NCPT15D	9	9	0:08	64K
MCHLKE4	X25	NCPT15D	9	9	0:08	9K
MCHLKE6	X25	NCPT15D	9	9	0:08	9K
MCHLK84A	X25	NCPT15D	9	9	0:08	64K

UNDER UTILIZED: LESS THAN OR EQUAL 7 PERCENT

Figure 3-

3.3.1.3.14 NPM/NetSpy Link Ranking By (Zone/Hour)

INTENDED USE:

To rank all or selected links in ascending or descending order based on sending, receiving, or total percent link busy. The user chooses the number of links to rank, the ranking order, and the ranking variable. The report provides both utilization and workload information that you can use to identify either overutilized or underutilized links.

FORMAT:

A 15 column report approximately 132 characters wide. It is best suited for hardcopy review but can be reviewed online. The information is summarized and presented by NETWRKID, SYSID, Data Range, and Zone or Zone by Hour.

INQUIRY ID:

SNTLDX - By Zone
SNTLDY - By Zone and Hour

DATA SOURCE (File/Timespan):

SNTNCL - Days

DATA ELEMENTS USED:

DURATION, HOUR, NETNAME, NCLPCLBS, NCLPCSBS, ZONE,
LINKSPD, NCLNRCHR, NCLNRCHS, NCLNRRLS, NCLNRSLS,
NCLNRERR, NCLNRRBY, NCLPCRLB, NCLPCSLB, NCLNRFRR,
NCLNRFRRS, NCLNRCON, NCLNRALC, DATATYPE

CALCULATIONS:

None

USAGE CONSIDERATIONS:

All cycles included are summarized together as a data range and reported at that granularity, either zone or hour within zone.

1

(SNTLDX) DAILY SNA LINK RANKING BY ZONE																
FIRST 25 SNA LINKS BY DESCENDING PERCENT LINK (LINE) BUSY																
NETWORK ID: NETWORK1			SYSTEM ID: SYS1			DATA RANGE: 040CTyy-17JUNyy										ZONE: 1
IDENTIFICATION				% LINK BUSY				WORKLOAD INFORMATION								
LINK	NCP	DURATION	LINK	-- TOTAL BYTES --				TOTAL MESSAGES				RXMIT RXMIT		TOTAL ERROR		OUTB QUEUE
NAME	NAME	(HH:MM)	SPEED	SEND	RECEV	TOTAL	SENT	RECD	TRANS	SENT	RECD	TRANS	MSG	BYTES	COUNTS	LENGTH
L2A216	GWN2AM	1:00	56K	55.68	2.416	58.10	14M	608K	14M	5K	6K	12K	0	0	0	0
L2A220	GWN2AM	1:00	56K	55.39	.9314	56.32	13M	234K	14M	5K	407	5K	0	0	0	0
L2A001	GWN2AM	1:00	9K	44.12	3.839	47.96	1M	165K	2M	10K	8K	19K	0	0	0	5
L12161	PEP12E	1:00	9K	35.35	6.616	41.97	1M	285K	1M	7K	4K	12K	0	0	0	6
L2A178	GWN2AM	1:00	9K	27.23	2.376	29.61	1M	102K	1M	6K	3K	10K	0	0	0	4
L2A154	GWN2AM	1:00	9K	17.11	3.172	20.28	738K	137K	875K	3K	1K	5K	0	0	0	0
L12182	PEP12E	1:00	9K	16.66	3.074	19.73	719K	132K	852K	3K	1K	5K	0	0	0	4
L12187	PEP12E	1:00	9K	15.66	3.328	18.98	676K	143K	820K	3K	1K	4K	0	0	0	0
L12046	PEP12E	1:00	7K	14.76	3.773	18.53	478K	122K	600K	1K	869	2K	0	0	0	0
L12183	PEP12E	1:00	9K	15.40	2.916	18.31	665K	125K	791K	2K	1K	3K	0	0	0	0
L12146	PEP12E	1:00	4K	11.16	5.256	16.41	241K	113K	354K	845	590	1K	0	0	0	0
L12023	PEP12E	1:00	9K	12.74	3.500	16.23	550K	151K	701K	2K	1K	3K	0	0	0	0
L12031	PEP12E	1:00	9K	11.67	2.771	14.44	503K	119K	623K	1K	545	2K	0	0	0	0
L12180	PEP12E	1:00	9K	9.953	2.645	12.60	429K	114K	544K	1K	875	2K	0	0	0	3
L12000	PEP12E	1:00	9K	9.598	2.920	12.52	414K	126K	540K	2K	1K	3K	0	0	0	0
L2A146	GWN2AM	1:00	9K	3.191	9.155	12.35	137K	395K	533K	799	1K	1K	0	0	0	0
L2A185	GWN2AM	1:00	19K	10.44	1.554	11.99	901K	134K	1M	2K	1K	4K	300	106K	565	1
L12189	PEP12E	1:00	9K	8.693	2.831	11.52	375K	122K	497K	1K	675	2K	0	0	0	0
L12042	PEP12E	1:00	4K	6.420	5.000	11.42	138K	107K	246K	183	84	267	0	0	0	0
L2A049	GWN2AM	1:00	9K	5.848	5.243	11.09	252K	226K	479K	315	310	625	0	0	0	0
L12050	PEP12E	1:00	9K	5.243	5.848	11.09	226K	252K	479K	310	315	625	0	0	0	0
L2A208	GWN2AM	1:00	56K	3.463	6.537	10.00	872K	1M	2M	6K	9K	15K	0	0	0	0
L12158	PEP12E	1:00	4K	4.916	4.916	9.832	106K	106K	212K	0	0	0	0	0	55	0
L12181	PEP12E	1:00	9K	4.726	5.076	9.802	204K	219K	423K	549	758	1K	0	0	0	0
L2A212	GWN2AM	1:00	56K	8.011	1.061	9.072	2M	267K	2M	8K	4K	12K	0	0	0	0

DATES=NONE, TIME=(00:00-24:00), NOTE:(K=THOUSANDS M=MILLIONS), RANKING=NCLPCLBS=PERCENT LINK (LINE) BUSY
 RUN-DATE=Wed,Sep3,yy, TIMESpan=DETAIL, DBID=8, FILE=NCL
 INCLUDE=LINK=NONE, INCLUDE=NCP=NONE
 EXCLUDE=LINK=NONE, EXCLUDE=NCP=NONE
 INCLUDE=SYSID=CRP, PRODUCT=NPM, VERSION=0013

Figure 3-

New Topic

INTENDED USE:

This chart is used to determine the traffic fluctuation on a link over a period of 24 hours. This helps determine the need for changes to the configuration, such as the addition of links or an increase in the link speed.

FORMAT:

This display produces a vertical bar chart of the percentage link utilization by hour for an individual link.

INQUIRY ID:

Color Graphics: N/A

Printer Graphics: SNTPDOR

DATA SOURCE (File/Timespan):

SNTNCL01 - Previous day

DATA ELEMENTS USED:

HOURL, NETNAME, NCLPCLBS

CALCULATIONS:

None

USAGE CONSIDERATIONS:

This inquiry is produced from NetView Performance Monitor (NPM) network data or CA NetSpy NCP interface data. Percent Link Utilization is based on the specification of Link Speed in an NCP parameter. If the actual speed of the link differs from the speed specified for the NCP line definition, the percentage displayed on this inquiry will be in error.

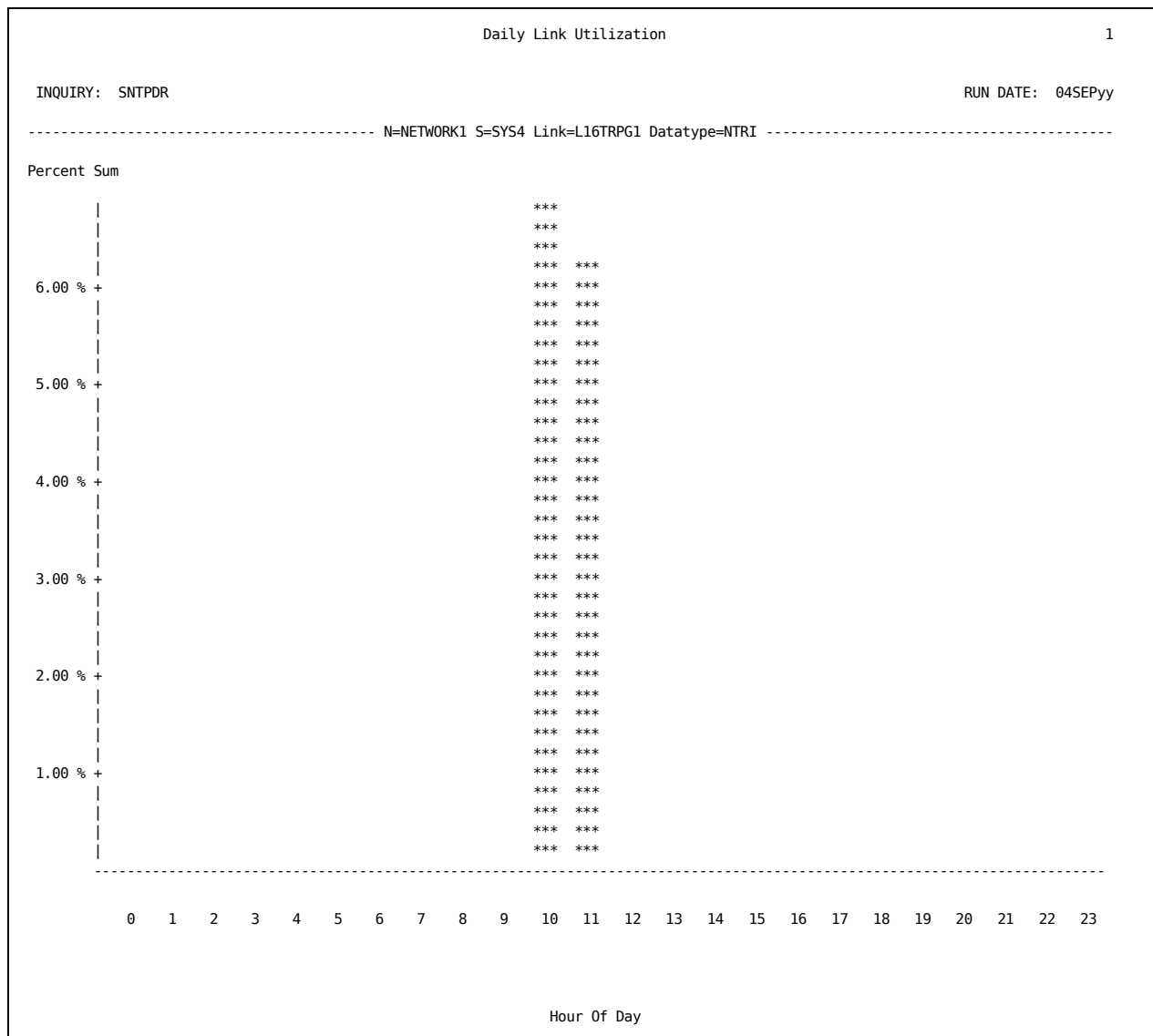


Figure 3-

3.3.1.4 Workload Analysis Inquiries

The workload analysis inquiries show character and message counts by primary logical unit (PLU), virtual routes, or site-defined account codes. Two rank reports are also included to identify links and applications having the largest average message sizes. Each inquiry is discussed in greater detail in the following sections:

- 1 - NetView Daily Connect Time by SNTACT1
- 2 - NetView Daily Chars/1000 by SNTACT1
- 3 - NetView Daily Data Chars/1000 by VR
- 4 - NetView Daily Data Chars/1000 by SNTACT1
- 5 - NetView Daily Cntl Chars/1000 by SNTACT1
- 6 - NetView Weekly Cntl PIU Traffic by PLU
- 7 - NetView Weekly Data PIU Traffic by PLU
- 8 - NetView Daily Link Rank Report
- 9 - NetView Daily PLU Rank Report
- 10 - NSA/NGA Daily Chars/1000 by SNTACT1
- 11 - NSA/NGA Daily PIU Traffic by SNTACT1
- 12 - NetSpy Daily Average VR Response Time

3.3.1.4.1 NetView Daily Connect Time by SNTACT1

INTENDED USE:

This chart displays the total network terminal connect hours for SNTACT1.

FORMAT:

This display produces a vertical bar chart of total connect hours by SNTACT1 by hour.

INQUIRY ID:

Color Graphics: SNTCDC

Printer Graphics: N/A

DATA SOURCE (File/Timespan):

NVSNSC01 - Previous day

DATA ELEMENTS USED:

SNTACT1, NSCCONTM

CALCULATIONS:

To convert NSCCONTM to the number of connect hours from a SAS time format, NSCCONTM is divided by 3600.

USAGE CONSIDERATIONS:

This inquiry is produced from NetView accounting and availability data. When you use the default value of SNTACT1, which is an account code that determines the summarization sequence of the file, a separate report is generated for each primary logical unit (PLU). If your data center has assigned a different value to SNTACT1, a new report will be produced for each unique occurrence of the value assigned to SNTACT1. Refer to the data element list in Chapter 5 for the NVSNCS File to find the value assigned to SNTACT1 at your site.

3.3.1.4.2 NetView Daily Chars/1000 by SNTACT1

INTENDED USE:

This chart displays the volume of data character traffic for each SNTACT1. You can use it to determine traffic workloads placed on the network by the total traffic to and from a given application.

FORMAT:

This display produces a vertical bar chart of total characters transmitted (sent and received) by SNTACT1.

INQUIRY ID:

Color Graphics: SNTCDD

Printer Graphics: N/A

DATA SOURCE (File/Timespan):

NVSNSC01 - Previous day

DATA ELEMENTS USED:

HOURL, SNTACT1, NSCNRTCH

CALCULATIONS:

To express character volume in kilo characters (characters/1000), the data element Total Characters Transmitted (NSCNRTCH) is divided by 1000.

USAGE CONSIDERATIONS:

This inquiry is produced from NetView accounting and availability data. When you use the default value of SNTACT1, which is an account code that determines the summarization sequence of the file, a separate report is generated for each primary logical unit (PLU). If your data center has assigned a different value to SNTACT1, a new report will be produced for each unique occurrence of the value assigned to SNTACT1. Refer to the data element list in Chapter 5 for the NVSNSC File to find the value assigned to SNTACT1 at your site.

3.3.1.4.3 NetView Daily Data Chars/1000 by VR

INTENDED USE:

This chart shows traffic load variation on a virtual route over a period of 24 hours. Its primary use is for virtual route planning and load balancing during peak hours.

FORMAT:

This display produces a vertical bar chart of total characters transmitted (sent and received) by virtual route by hour.

INQUIRY ID:

Color Graphics: SNTCDE

Printer Graphics: N/A

DATA SOURCE (File/Timespan):

NVSRTE01 - Previous day

DATA ELEMENTS USED:

hour, RTEVRTTE RTENRTCH

CALCULATIONS:

To express character volume in kilo characters (characters/1000), the data element Total Characters Transmitted (RTENRTCH) is divided by 1000.

USAGE CONSIDERATIONS:

This inquiry is produced from NetView accounting and availability data.

3.3.1.4.4 NetView Daily Data Chars/1000 by SNTACT1

INTENDED USE:

This chart displays the volume of data character traffic for each SNTACT1. You can use it to pinpoint periods of peak activity that may be correlated with poor response time or periods of low activity, possibly indicating problems in the network or on the host.

FORMAT:

This display produces a stacked vertical bar chart of data characters transmitted (sent and received), grouped by hour.

INQUIRY ID:

Color Graphics: SNTCDF
Printer Graphics: N/A

DATA SOURCE (File/Timespan):

NVSNSA01 - Previous day

DATA ELEMENTS USED:

SNTACT1, NSANRTBS, NSANRTBR

CALCULATIONS:

To express character volume in kilo characters (characters/1000), the data elements Number of Text Bytes Sent (NSANRTBS) and Number of Text Bytes Received (NSANRTBR) are each divided by 1000.

USAGE CONSIDERATIONS:

This inquiry is produced from NetView accounting and availability data. When you use the default value of SNTACT1, which is an account code that determines the summarization sequence of the file, a separate report is generated for each primary logical unit (PLU). If your data center has assigned a different value to SNTACT1, a new report will be produced for each unique occurrence of the value assigned to SNTACT1. Refer to the data element list in Chapter 5 for the NVNSA File to find the value assigned to SNTACT1 at your site.

3.3.1.4.5 NetView Daily Cntl Chars/1000 by SNTACT1

INTENDED USE:

This chart displays control character traffic volume for each SNTACT1. You can compare it with the MICF inquiry SNTCDF, NetView Daily Dat Chars/1000 by SNTACT1, to determine the ratio between data and control characters.

FORMAT:

This display produces a stacked vertical bar chart of control characters transmitted (sent and received), grouped by hour.

INQUIRY ID:

Color Graphics: SNTCDG
Printer Graphics: N/A

DATA SOURCE (File/Timespan):

NVSNSA01 - Previous day

DATA ELEMENTS USED:

SNTACT1, NSANRCBS, NSANRCBR

CALCULATIONS:

To express character volume in kilo characters (characters/1000), the data elements Number of Control Bytes Sent (NSANRCBS) and Number of Control Bytes Received (NSANRCBR) are each divided by 1000.

USAGE CONSIDERATIONS:

This inquiry is produced from NetView accounting and availability data. When you use the default value of SNTACT1, which is an account code that determines the summarization sequence of the file, a separate report is generated for each primary logical unit (PLU). If your data center has assigned a different value to SNTACT1, a new report will be produced for each unique occurrence of the value assigned to SNTACT1. Refer to the data element list in Chapter 5 for the NVSNSA File to find the value assigned to SNTACT1 at your site.

3.3.1.4.6 NetView Weekly Cntl PIU Traffic by PLU

INTENDED USE:

This chart displays control message volumes for individual PLUs. You can compare it with the MICF inquiry SNTCWK, NetView weekly data PIU traffic by PLU, to determine the ratio between data and control PIUs.

FORMAT:

This display produces a stacked vertical bar chart of control path information units (PIUs) transmitted (sent and received) by primary logical unit (PLU).

INQUIRY ID:

Color Graphics: SNTCWH

Printer Graphics: N/A

DATA SOURCE (File/Timespan):

NVSLSY01 - Previous day

DATA ELEMENTS USED:

HOURL, PLU, LSYNRCPS, LSYNRCPR

CALCULATIONS:

NONE

USAGE CONSIDERATIONS:

This inquiry is produced from NetView accounting and availability data.

3.3.1.4.7 NetView Weekly Data PIU Traffic by PLU

INTENDED USE:

This chart displays data message volumes for individual PLUs. You can use it to determine traffic workloads imposed by individual applications on the network.

FORMAT:

This display produces a stacked vertical bar chart of data path information units (PIUs) transmitted (sent and received) by primary logical unit (PLU).

INQUIRY ID:

Color Graphics: SNTCWK
Printer Graphics: N/A

DATA SOURCE (File/Timespan):

NVSLSY01 - Previous day

DATA ELEMENTS USED:

HOURL, PLU, LSYNRTPS, LSYNRTPR

CALCULATIONS:

NONE

USAGE CONSIDERATIONS:

This inquiry is produced from NetView accounting and availability data.

3.3.1.4.8 NetView Daily Link Rank Report

INTENDED USE:

This report identifies links that have long average message lengths.

FORMAT:

This display produces a rank report of the ten links with the longest average message length. These links are listed in descending order from the longest average message length sent from the host. It also lists the SLU subarea physical unit (SLUSAPU), the NCP to which the link is attached.

INQUIRY ID:

Color Graphics: N/A
Printer Graphics: SNTLDL

DATA SOURCE (File/Timespan):

NVSNLL01 - Previous day

DATA ELEMENTS USED:

NLLAVTBS, SLULINK, SLUSAPU

CALCULATIONS:

None

USAGE CONSIDERATIONS:

You can use this report in conjunction with MICF inquiry SNTLDM, NetView Daily PLU Rank Report, to identify interactive applications and terminal devices that can potentially monopolize line capacity due to long message sizes.

10 Links With Longest Avg Message Length				1
INQUIRY: SNTLDL		RUN DATE: 03SEPy		
----- N=NETWORK1 S=SCNN -----				
Average Bytes per PIU Sent (Text)	SLU Link	SLU Subarea Physical Unit	Primary Logical Unit	
1156.00	L170170	N170L9	H059CSM1	
1156.00	L170164	N170L9	H059CSM1	
1156.00	L368026	N368L7	H059CSM1	
1156.00	L368009	N368L7	H059CSM1	
900.00	L152064	N152L0	H059CSM3	
746.25	L170166	N170L9	H059CSM1	
667.50	L368016	N368L7	H059CSM1	
667.50	L368029	N368L7	H059CSM1	
650.25	L368004	N368L7	H059CSM1	
591.00	L368003	N368L7	H059CSM1	
----- N=NETWORK1 S=SYSB -----				
Average Bytes per PIU Sent (Text)	SLU Link	SLU Subarea Physical Unit	Primary Logical Unit	
1084.32	NC000023	C50NCP8	CICSA	
1010.48	0A24	HOST42	VCISYS1A	
926.88	CC000123	C50NCP8	CGATE7	
777.50	CC000124	C50NCP8	CGATE7	
777.50	CC000015	C50NCP8	CGATE6	
734.14	0C12	HOST42	C02CMS	
709.79	CC000063	C50NCP8	C41TS061	
703.76		HOST42	WKMGR001	
692.83	CC000066	C48NCP1	VPS001	
692.24	0A23	HOST42	NET42015	

Figure 3-

3.3.1.4.9 NetView Daily PLU Rank Report

INTENDED USE:

Long average message lengths combined with high message rates can dramatically affect network response time. This report identifies applications that might benefit most from adjusting parameters to reduce message sizes or from compression software.

FORMAT:

This display produces a rank report of the five primary logical units (PLUs) having the longest average message length. These PLUs are listed in descending order from the longest average message length sent from the host. The host system identifier and the network identifier are also listed.

INQUIRY ID:

Color Graphics: N/A
Printer Graphics: SNTLDM

DATA SOURCE (File/Timespan):

NVSNLL01 - Previous day

DATA ELEMENTS USED:

LSYAVTBS, PLU, SYSID, NETWRKID

CALCULATIONS:

None

USAGE CONSIDERATIONS:

You can use this report in conjunction with MICF inquiry SNTLDL, NetView Daily Link Rank report, to identify interactive applications and terminal devices that can potentially monopolize line capacity due to long message sizes.

5 PLUs With Longest Average Message Length		1
INQUIRY: SNTLDM	RUN DATE: 03SEPyy	
----- N=NETWORK1 S=SCNN -----		
Average Bytes per PIU Sent (Text)	Primary Logical Unit	
900.0	H059CSM3	
710.6	H059CSM1	
409.6	H059CSM4	
235.0	H0ST184	
234.0	H0ST67	
----- N=NETWORK1 S=SYSB -----		
Average Bytes per PIU Sent (Text)	Primary Logical Unit	
1322.4	VCISYSN3	
1085.1	WIZ	
1011.5	VCISYS1A	
912.2	C41TS102	
902.2	C41TS305	

Figure 3-

3.3.1.4.10 NSA/NGA Daily Chars/1000 by SNTACT1

INTENDED USE:

This chart displays the volume of character traffic for each SNTACT1. You can use it to pinpoint periods of peak activity that may be correlated with poor response time or periods of low activity, possibly indicating problems in the network or on the host.

FORMAT:

This display produces a stacked vertical bar chart of characters transmitted (sent and received), grouped by hour.

INQUIRY ID:

Color Graphics: SNTCDX
Printer Graphics: SNTPDY

DATA SOURCE (File/Timespan):

SNTNAC01 - Previous day

DATA ELEMENTS USED:

SNTACT1, HOUR, NACNRTBS, NACNRTBR, NACNRCBS, NACNRCBR

CALCULATIONS:

To chart total characters sent and total characters received, text character counts (NACNRTBS and NACNRTBR) and control character counts (NACNRCBS and NACNRCBR) are combined for each direction. These resulting sums are divided by 1000 to express character volume in kilo characters.

USAGE CONSIDERATIONS:

This inquiry is produced from either CA NetSpy or NPM network session accounting/network gateway accounting data. When you use the default value of SNTACT1, which is an account code that determines the summarization sequence of the file, a separate report is generated for each primary logical unit (PLU). If your data center has assigned a different value to SNTACT1, a new report will be produced for each unique occurrence of the value

assigned to SNTACT1. See the data element list in Chapter 5 for the SNTNAC file to find the value assigned to SNTACT1 at your site.

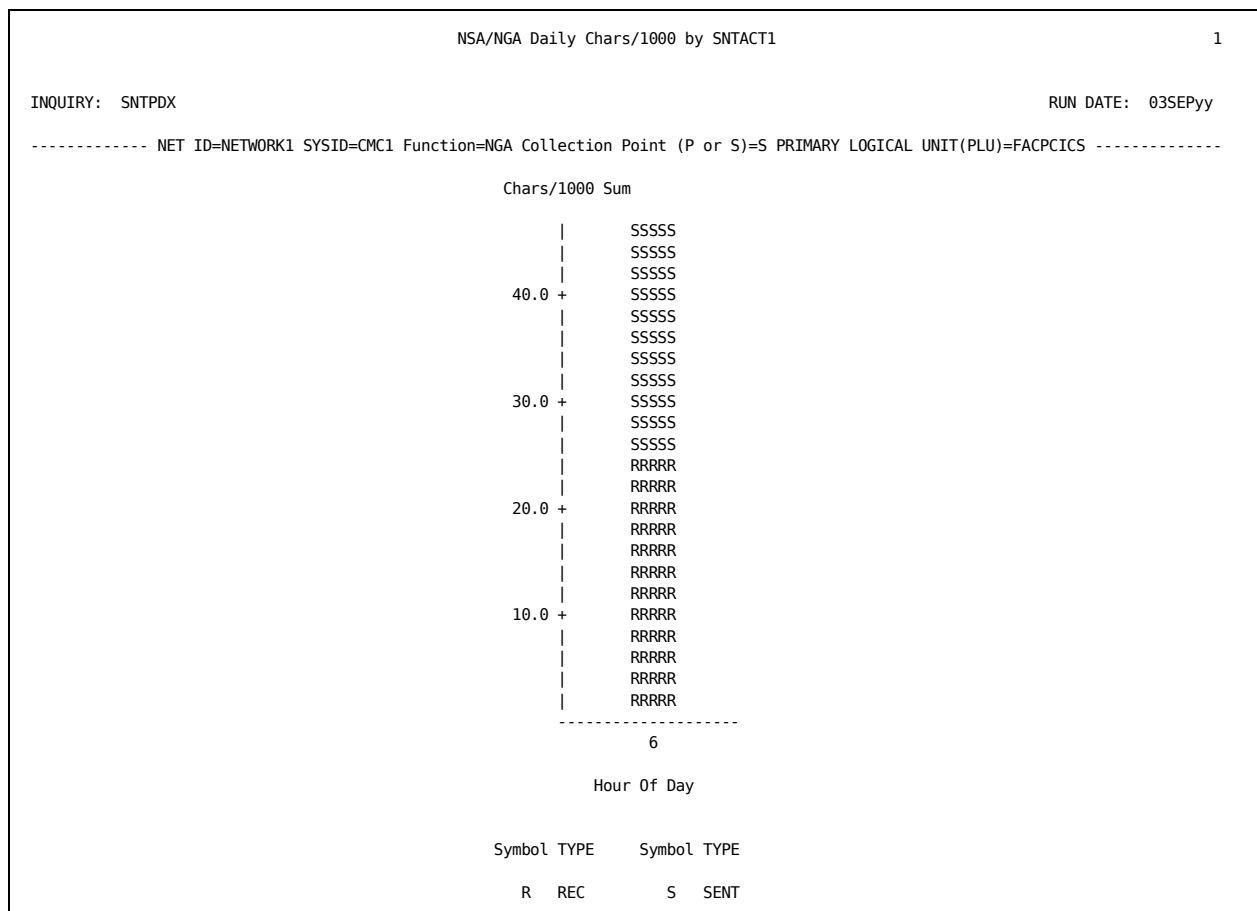


Figure 3-

3.3.1.4.11 NSA/NGA Daily PIU Traffic by SNTACT1

INTENDED USE:

This chart displays PIU (message) volumes for each SNTACT1. You can use it to pinpoint periods of peak activity that may be correlated with poor response time or periods of low activity, possibly indicating problems in the network or on the host.

FORMAT:

This display produces a stacked vertical bar chart of PIUs transmitted (sent and received), grouped by hour.

INQUIRY ID:

Color Graphics: SNTCDY
Printer Graphics: SNTPDY

DATA SOURCE (File/Timespan):

SNTNAC01 - Previous day

DATA ELEMENTS USED:

SNTACT1, HOUR, NACNRCPS, NACNRCPR, NACNRTPR, NACNRTPS

CALCULATIONS:

To chart total PIUs sent and total PIUs received, text PIU counts (NACNRTPS and NACNRTPR) and control PIU counts (NACNRCPS and NACNRCPR) are combined for each direction.

USAGE CONSIDERATIONS:

This inquiry is produced from either CA NetSpy or NPM network session accounting/network gateway accounting data. When you use the default value of SNTACT1, which is an account code that determines the summarization sequence of the file, a separate report is generated for each primary logical unit (PLU). If your data center has assigned a different value to SNTACT1, a new report will be produced for each unique occurrence of the value assigned to SNTACT1. Refer to the data element list in Chapter 5 for the SNTNAC File to find the value assigned to SNTACT1 at your site.

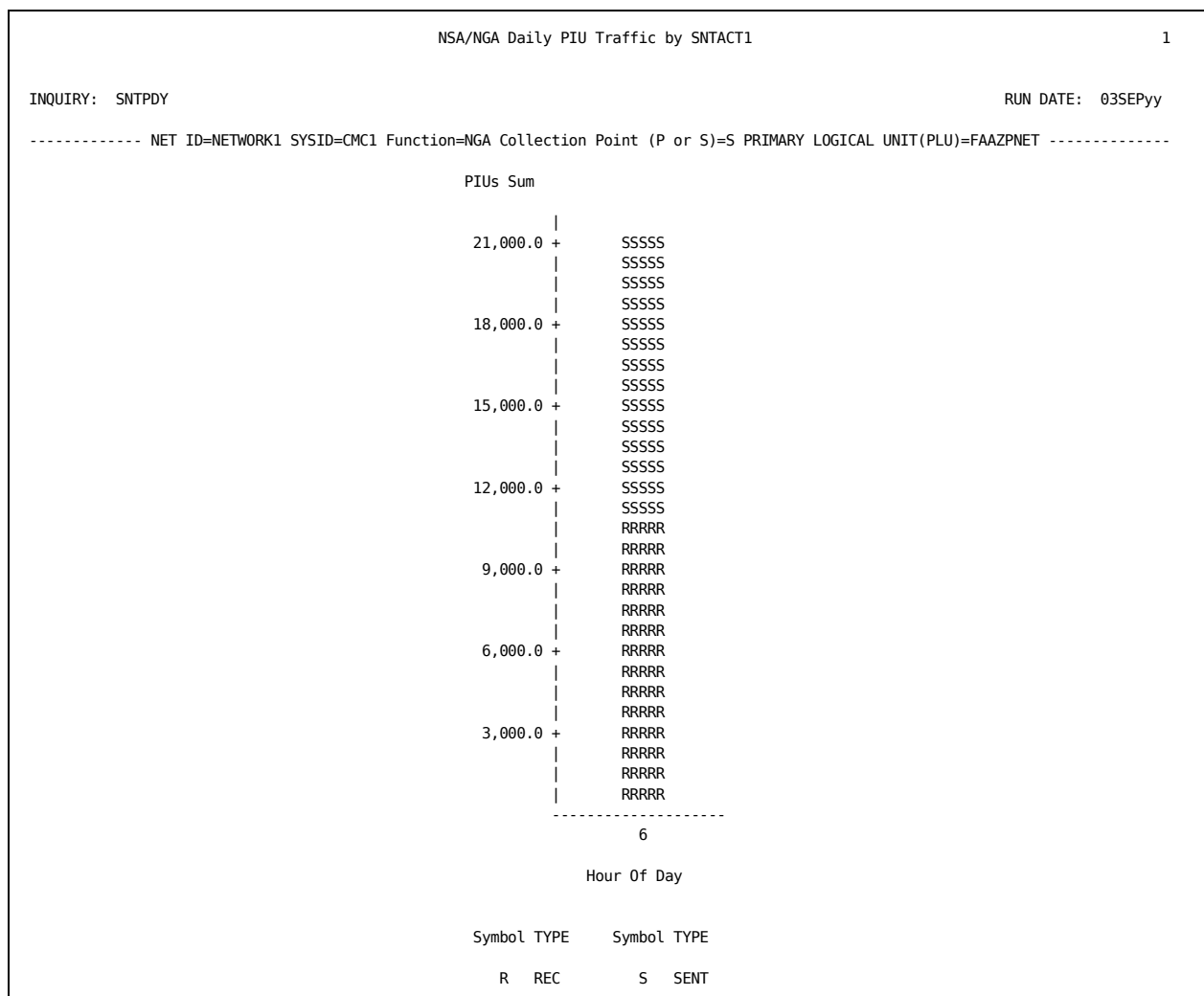


Figure 3-

3.3.1.5 Resource Analysis Inquiries

The Resource analysis inquiries show In Byte Count and Out Byte Count. The daily reports present byte count by the hour and monthly reports present byte count by zone. Two extract reports are provided to generate daily and monthly byte count Comma Separated Value (CSV) files that you can use to display color graphics on the workstation using CA MICS Q&R WorkStation. Each inquiry is discussed in greater detail in the following sections:

- 1 - TCP/IP Daily In Byte Count By Hour
- 2 - TCP/IP Daily Out Byte Count By Hour
- 3 - TCP/IP Monthly In Byte Count By Zone
- 4 - TCP/IP Monthly Out Byte Count By Zone
- 5 - TCP/IP Daily Bytes Trans./Hour (CSV)
- 6 - TCP/IP Daily Bytes Trans./Hour (CSV)

3.3.1.5.1 TCP/IP Daily In Byte Count By Hour

INTENDED USE:

This chart displays the TCP/IP Telnet Server (TCPSTN) file's data element, In Byte Count (STNBYTEI), sorted by hour within a day for each sysid.

FORMAT:

This display produces a vertical bar chart of In Byte Count each hour.

INQUIRY ID:

Color Graphics: N/A

Printer Graphics: SNTPD2

DATA SOURCE (File/Timespan):

TCPSTN01 - Previous day

DATA ELEMENTS USED:

SYSID, DAY, HOUR, and STNBYTEI

CALCULATIONS:

None.

USAGE CONSIDERATIONS:

None.

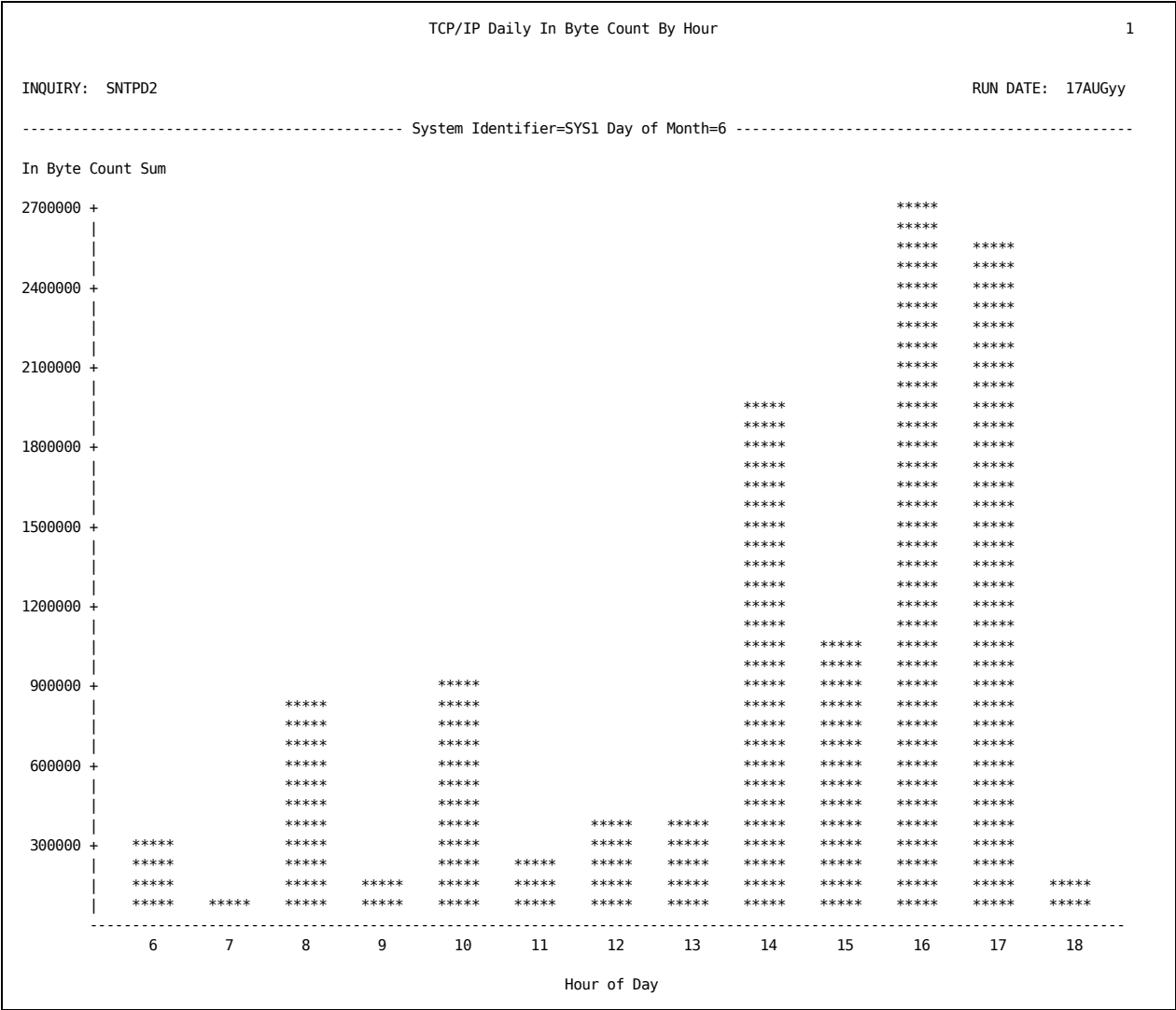


Figure 3-

3.3.1.5.2 TCP/IP Daily Out Byte Count By Hour

INTENDED USE:

This chart displays the TCP/IP Telnet Server (TCPSTN) file's data element, Out Byte Count (STNBYTE0), sorted by hour within a day for each sysid.

FORMAT:

This display produces a vertical bar chart of Out Byte Count by hour.

INQUIRY ID:

Color Graphics: N/A
Printer Graphics: SNTPD3

DATA SOURCE (File/Timespan):

TCPSTN01 - Previous day

DATA ELEMENTS USED:

SYSID, DAY, HOUR, and STNBYTE0

CALCULATIONS:

None.

USAGE CONSIDERATIONS:

None.

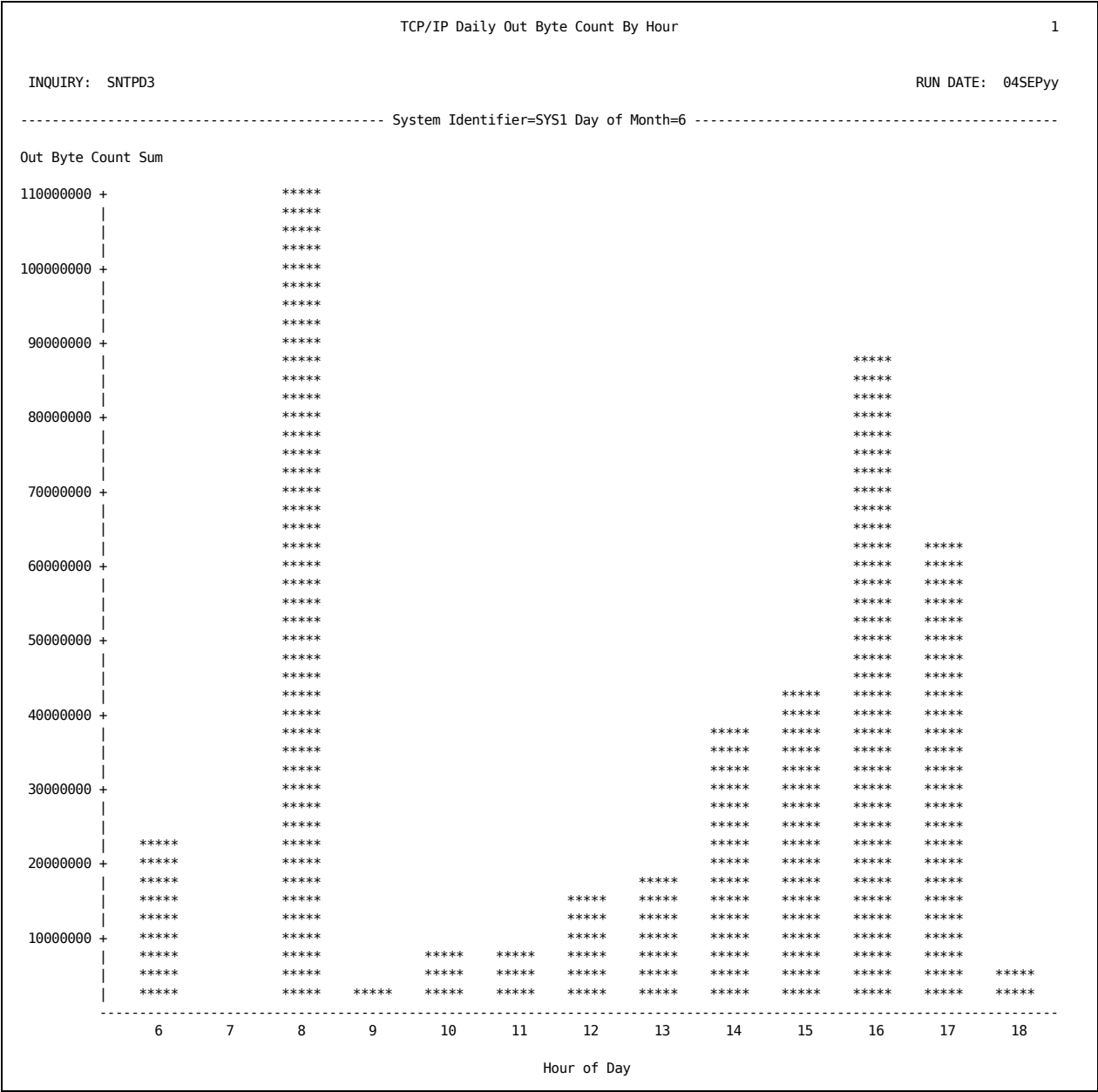


Figure 3-

3.3.1.5.3 TCP/IP Monthly In Byte Count By Zone

INTENDED USE:

This chart displays the TCP/IP Telnet Server (TCPSTN) file's data element, In Byte Count (STNBYTEI), sorted by zone within a month for each sysid.

FORMAT:

This display produces a vertical bar chart of In Byte Count by zone.

INQUIRY ID:

Color Graphics: N/A

Printer Graphics: SNTPM1

DATA SOURCE (File/Timespan):

TCPSTN00 - Current Month

DATA ELEMENTS USED:

SYSID, MONTH, ZONE, and STNBYTEI

CALCULATIONS:

None.

USAGE CONSIDERATIONS:

None.

Figure 3-

3.3.1.5.4 TCP/IP Monthly Out Byte Count By Zone

INTENDED USE:

This chart displays the TCP/IP Telnet Server (TCPSTN) file's data element, Out Byte Count (STNBYTE0), sorted by zone within a month for each sysid.

FORMAT:

This display produces a vertical bar chart of Out Byte Count by zone.

INQUIRY ID:

Color Graphics: N/A
Printer Graphics: SNTPM2

DATA SOURCE (File/Timespan):

TCPSTN00 - Current Month

DATA ELEMENTS USED:

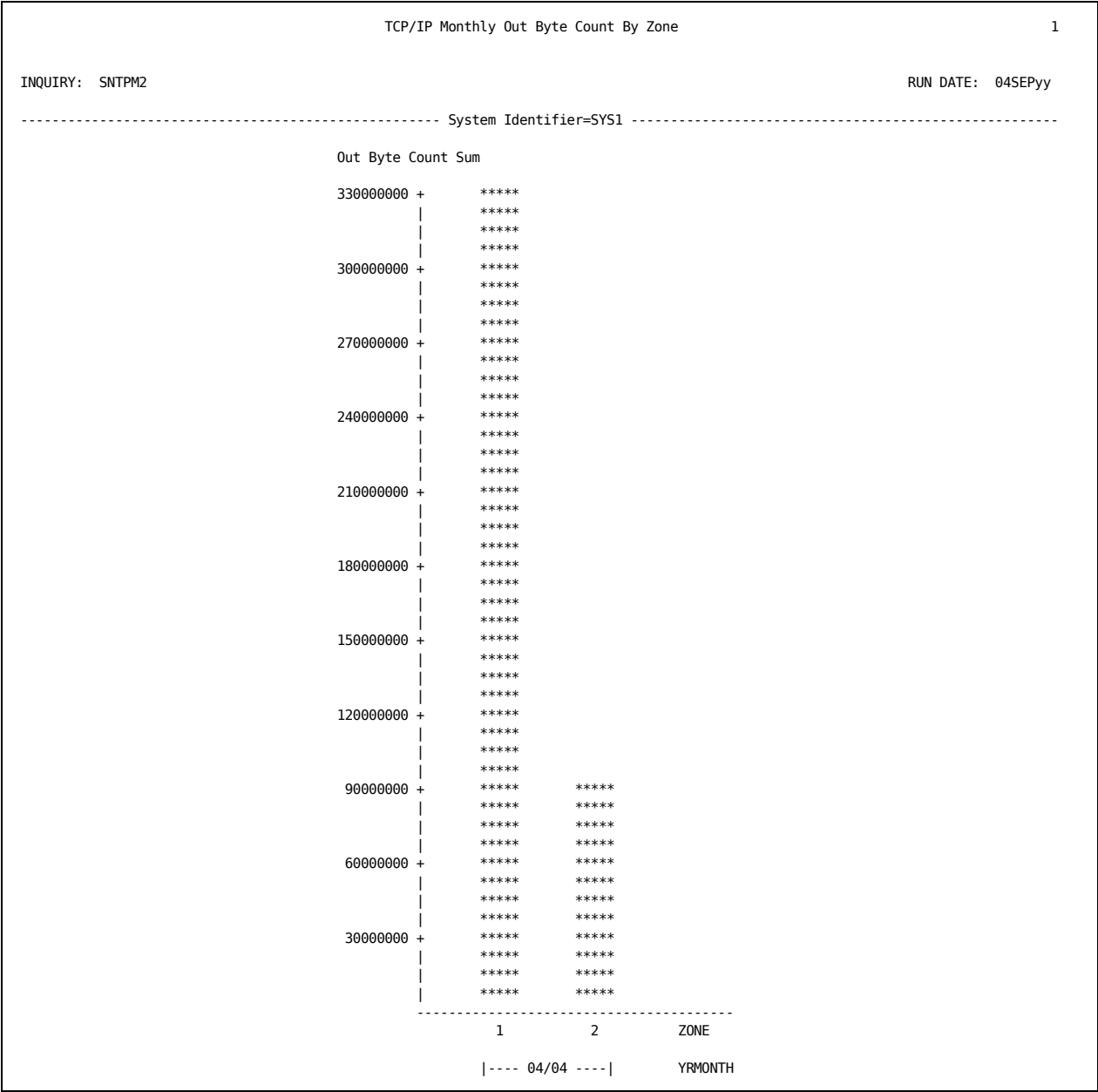
SYSID, MONTH, ZONE, and STNBYTE0

CALCULATIONS:

None.

USAGE CONSIDERATIONS:

None.



sntpm2s

Figure 3-

3.3.1.5.5 TCP/IP Daily Bytes Trans./Hour (CSV)

INTENDED USE:

This inquiry creates a CSV file that can be extended to CA MICS Q&R Workstation. The CSV data is taken from the TCP/IP Telnet Server (TCPSTN) file's data elements, In Byte Count (STNBYTEI) and Out Byte Count (STNBYTEO), sorted by hour within a day for each sysid. The CSV output can be used to generate graphs that analyze telnet server usage.

FORMAT:

Comma Separated Value (CSV) file.

INQUIRY ID:

Color Graphics: N/A
Printer Graphics: N/A

DATA SOURCE (File/Timespan):

TCPSTN01 - Previous day

DATA ELEMENTS USED:

SYSID, DAY, HOUR, STNBYTEI, and STNBYTEO

CALCULATIONS:

None.

USAGE CONSIDERATIONS:

None.

3.3.1.5.6 TCP/IP Monthly Bytes Trans./Zone (CSV)

INTENDED USE:

This inquiry creates a CSV file that can be extended to CA MICS Q&R Workstation. The CSV data is taken from the TCP/IP Telnet Server (TCPSTN) file's data elements, In Byte Count (STNBYTEI) and Out Byte Count (STNBYTEO), sorted by zone by month for each sysid. The CSV output can be used to generate graphs that analyze telnet server usage.

FORMAT:

Comma Separated Value (CSV) file.

INQUIRY ID:

Color Graphics: N/A
Printer Graphics: N/A

DATA SOURCE (File/Timespan):

TCPSTN01 - Previous day

DATA ELEMENTS USED:

SYSID, DAY, HOUR, STNBYTEI, and STNBYTEO

CALCULATIONS:

None.

USAGE CONSIDERATIONS:

None.

3.3.2 How to Modify Standard MICF Inquiries

See the MICF Tutorial in the MICF User Guide for information on modifying cataloged inquiries.

You may want to tailor the distributed MICF inquiries for your installation, and particularly to change the labels of subtitle headings for the distributed inquiries for files with user-defined account codes in the NVS Information Area (for example, NVSRTM and NVSNSA). The inquiries for these files generate graphs or reports for the value of each account code. The account codes are labeled on the graphs by generic name (for example, SNTACT1). The inquiry SNTCDF, for example, provides a stacked vertical bar chart of data character traffic (by direction) for each unique value of SNTACT1 in the NVSNSA File if your installation has assigned a specific network component type, such as primary logical unit (PLU), to be the value of SNTACT1. The procedure below identifies the steps you must follow to change titles and subtitles to reflect your installation's choice for SNTACT1. Assuming that SNTACT1 contains PLU, this procedure shows you how to change SNTACT1 to PLU.

- 1 - Determine the value assigned to SNTACT1 at your site by referring to the NVSNSA data element list in Chapter 5. Verify with your CA MICS System Administrator that the value is correct.
- 2 - Copy the inquiry from the MICF shared catalog to your private catalog and change the inquiry name. (See Figure 3-36.)
- 3 - For this example, we have changed the inquiry's name to SNT001. Enter the author's name. Change the title to NetView Daily Chars/1000 by PLU by overkeying the current title. (See Figure 3-36A.)
- 4 - Select Modify Mode by typing MODIFY in the Select Mode field. Select the new inquiry by typing an S opposite the name of the inquiry you want to modify. (See Figure 3-36B.)
- 5 - Select Color Vertical Bar Chart by typing an S opposite that field. (See Figure 3-36C.)
- 6 - Enter a Y in the extended options field at the bottom of the screen. Change the report title to NetView Daily Chars/1000 by PLU by overkeying the current title. (See Figure 3-36D.)

- 7 - Enter a Y opposite the Specify Subheading Text and Data Formats field. (See Figure 3-36E.)
- 8 - Type PLU in the Subheading Text field for the element SNTACT1. (See Figure 3-36F.)
- 9 - Type END at the command prompt, pressing ENTER until you return to the MICF Inquiry Step Display screen. At the command prompt, type V and press ENTER to validate the inquiry that you just created. (See Figure 3-36G.) The message 'Inquiry Validated' will appear in the upper righthand corner of the screen (not shown).

- 10 - Type END at the command prompt and you will be prompted by the Active Inquiry Save Confirmation screen to 'Press ENTER key to save the current, active MICF Inquiry'. Press ENTER and you will return to the Data Base Inquiries screen. (See Figure 3-36H.)
- 11 - Select Execute Mode by typing EXECUTE in the Select Mode field, then type an S opposite the inquiry that you just created and modified to execute it. (See Figure 3-36I.)

```

/-----\
|----- Data Base Inquiries -----|
|Command ==>                               Scroll ==> PAGE |
|
|Catalog    ==> SHARED (PRIVATE/SHARED) Catalog Group    ==> * |
|Select Mode ==> EXECUTE (EXECUTE/MODIFY) Name (subset display) ==> _____ |
|
|Line Cmds: S Select  I Insert   R Repeat  C Copy   D Delete |
|
|Cmd  Name                Title                Date    Time |
| -  - - - - - - - - - - - - - - - - - - - - - - - - - - - - |
| -  SNTCDC  NetView Daily Connect Time by SNTACT1    87/05/08  17:00 |
| C  SNTCDD  NetView Daily Chars/1000 by SNTACT1      87/05/08  17:05 |
| -  SNTCDE  NetView DAily Chars/1000 by VR           87/05/08  17:10 |
|
|
|
|
|
|
|***** BOTTOM OF DATA *****|
[assign the value for vfor in your
book]-----[assign the
value for vinf in your book]

```

Figure 3-36. Copying an Inquiry to a Private Catalog

```
[assign the value for vfor in your
book]-----[assign the
value for vinf in your book]
```

```

/-----\
|----- Data Base Inquiries -----|
|Command ==>                               Scroll ==> PAGE |
|
|Catalog    ==> PRIVATE (PRIVATE/SHARED)  Catalog Group    ==> * |
|Select Mode ==> MODIFY (EXECUTE/MODIFY)  Name (subset display) ==> _____ |
|
|Line Cmds: S Select  I Insert   R Repeat  C Copy   D Delete |
|
|Cmd  Name                Title                Date      Time |
| -  - - - - - - - - - - - - - - - - - - - - - - - - - - - - |
| S   SNT001  NetView Daily Chars/1000 by PLU      87/05/08   17:05 |
|
|
|
|
|
|
|***** BOTTOM OF DATA *****|
[assign the value for vfor in your
book]-----[assign the
value for vinf in your book]

```

Figure 3-36B. Selecting an Inquiry for Modification


```

/----- Color Vertical Bar Chart -----|
|Command ==>|
|Enter a ? in any data entry field for more information on valid values.|
|Modifying CA MICS Inquiry: SNT001 - NetView Daily Chars/1000 by PLU|
|Inquiry Step ==> Color Vertical Bar Chart - Chars/1000 by HOUR|
|Input File ==> FILE1 - Intermediate File Number 1 (From: DAYS NSC )|
|Report Title ==> NetView Daily Chars/1000 by PLU|
|
|Chart of ==> CHARS (Y-Axis) Grouped by ==> (Element)|
|Charted by ==> HOUR (X-Axis) Weighted by ==> (Element)|
|Type of Chart ==> SUM (SUM/MEAN/FREQ/PCT)|
|
|Generate Graph for Each Value of ==> NETWRKID _ SYSID__ _ SNTACT1_ _|
|-----|
|
|Graph a Discrete X-Axis ==> Y (Y/N) X-Axis Bar Size Sequence ==> _ (A/D)|
|Graph Cumulative Values ==> N (Y/N)|
|
|
|Specify Extended Options ==> Y (Y/N) ** Specified **|
|assign the value for vfor in your|
book]-----[assign the
value for vinf in your book]

```

Figure 3-36D. Specifying Extended Options

```
/-----\
|----- Extended Options Menu -----|
|Command ==>                          |
|Inquiry Step: Color Vertical Bar Chart - Characters/1000 by HOUR |
|Input File:   File1 - Intermediate File Number 1 (From: DAYS NSC)|
|Specify Data Element Labels and Formats      ==> N (Y/N/R)  ** Specified ** |
|Specify Subheading Text and Data Formats     ==> Y (Y/N/R)  ** Specified ** |
|Specify Axis Scale                          ==> N (Y/N/R)  ** Specified ** |
|Specify Reference Lines                     ==> N (Y/N/R) |
|Specify Chart Group Values                  ==> N (Y/N/R) |
|
|
|
|
|
|
|
|
|Begin Chart With Record Number ==> _____ Stop After ==> _____ Records |
|assign the value for vfor in your book]-----[assign the
value for vinf in your book]
```

Figure 3-36E. Selecting a Specify Option

```
/-----\
|-----Subheading Text and Data Formats-----|
|Command ===>|
|
|Inquiry Step: Color Vertical Bar Chart - Characters/1000 by HOUR|
|Input File:   File1 - Intermediate File Number 1 (From: DAYS NSC)|
|
|Element          Subheading Text          Output Format|
|-----|-----|-----|
|NETWRKID    N                               $CHAR8.|
|SYSID       S                               $CHAR4.|
|SNTACT1     PLU                             |
|
|
|
|
|
|
|
|
|
|[assign the value for vfor in your book]-----[assign the
value for vinf in your book]
```

Figure 3-36F. Specifying Subheading Text in Extended Options


```

/-----\
|----- MICF Inquiry Step Display -----|
|Command ==> V                               Scroll ==> CSR |
|
|Modifying CA MICS Inquiry: SNT001 - NetView Daily Chars/1000 by PLU |
|Inquiry validation is required. Enter VALIDATE to validate the inquiry. |
|Execute the Inquiry in ==> FOREGROUND (BATCH/FOREGROUND) Mode ==> N (Y/N) |
|
|Line Cmds: S Select  I Insert  D Delete  M Move  R Repeat  C Copy |
|
|Cmd          Inquiry Step          Input File |
| - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - |
| -  CA MICS File Selection          DAYS NSC |
| -  Common Data Selection - Select Previous Day  FILE1 |
| -  Execution-Time Data Selection - Select NETWRKID  FILE1 |
| -  Execution-Time Data Selection - Select SYSID    FILE1 |
| -  Execution-Time Data Selection - Select SNTACT1  FILE1 |
| -  Data Element Derivation - Characters/1000      FILE1 |
| -  Color Vertical Bar Chart - Characters/1000 by HOUR  FILE1 |
|
|***** BOTTOM OF DATA *****|
[assign the value for vfor in your
book]-----[assign the
value for vinf in your book]

```

Figure 3-36G. Validating a Modified Inquiry

```
/-----\
|----- Active Inquiry Save Confirmation ----- Confirm Save. |
|Command ==>|
|
| Active MICF Inquiry: SNT001 - NetView Daily Chars/1000 by PLU |
| Author: Your Name |
|
| Do you wish to save the current, active MICF Inquiry? ==> YES (YES/NO) |
|
|
|
|Instructions:|
|
| Press ENTER key to save the current, active MICF Inquiry. |
|
| Reply NO and press ENTER key to delete the current, active inquiry. |
|
| [assign the value for vfor in your book]-----[assign the |
| value for vinf in your book]
```

Figure 3-36H. Saving a Modified Inquiry

```

/-----\
|----- Data Base Inquiries -----|
|Command ==>                               Scroll ==> PAGE|
|
|Catalog    ==> PRIVATE (PRIVATE/SHARED)  Catalog Group    ==> *|
|Select Mode ==> EXECUTE (EXECUTE/MODIFY)  Name (subset display) ==> _____|
|
|Line Cmds: S Select  I Insert   R Repeat   C Copy    D Delete|
|
|Cmd   Name                Title                Date      Time|
|-----|-----|-----|-----|-----|
|S    SNT001  NetView Daily Chars/1000 by PLU      87/05/08   17:05|
|
|
|
|
|
|
|
|
|***** BOTTOM OF DATA *****|
[assign the value for vfor in your
book]-----[assign the
value for vinf in your book]

```

Figure 3-36I. Selecting a Modified Inquiry for Execution

Chapter 4: EXCEPTION REPORTING

To pinpoint problem areas that may undermine an installation's effectiveness, CA MICS provides exception reporting. Exception reporting can report an occurrence that is a distinct problem (e.g., TCAM/VTAM outage at 2:00 PM), one that may be a problem and requires further research (e.g., TSO user overloaded the system from 1:00 to 1:30 PM), or one that represents a standard, security, or audit violation (e.g., user XYZ is not authorized to use SUPERZAP and was detected using it seven times last week).

This problem reporting is linked to the areas of installation management responsibility -- availability, service, workload, standards, security, and performance.

The exception reporting process uses threshold values, which are defined by the installation, to test for instances that do not conform to the values. These instances are called exceptions.

The process produces several standard reports. Some reports are produced from an option within the CA MICS daily update. These include the following:

- o Exception Management Overview

This is a count of the number of critical, impacting, and warning conditions.

- o Severity Level Exception Summary

This report lists the exceptions that were encountered by time of day and level of severity.

- o Management Area Exception Summary

This summary lists the exceptions for the day for each management area, listed by hour.

Exception DETAIL reports are produced via the CA MICS Information Center Facility (MICF). These reports are the following:

- o Full Exception DETAIL Report
- o Short Exception DETAIL Report

These reports detail the exceptions encountered, listing the threshold value that was set and the value that was encountered. They are used to diagnose the individual exceptions that occur.

This chapter describes the philosophy and requirements of exception reporting, the operational flow, the exceptions provided with this Analyzer, and a detailed explanation of the exception definition process.

This section contains the following topics:

- [4.1 Philosophy and Requirements](#) (see page 495)
- [4.2 Exception Processing](#) (see page 496)
- [4.3 Using the Exception Reports for Problem Analysis](#) (see page 497)
- [4.4 Identification and Qualification](#) (see page 498)
- [4.5 CA MICS Network Standard Exceptions List](#) (see page 502)
- [4.6 Detail Exception Descriptions](#) (see page 504)

4.1 Philosophy and Requirements

The technique of exception reporting has always had value for data processing management. The increase in growth and complexity of data processing data centers, however, makes exception reporting a necessity for even the smallest sites.

At z/OS data centers, the CPU processor or processor complex operates many types of systems software -- for example, SCP, TSO, JES2, batch, and TCAM. Each of these must frequently perform a significant level of processing. This combination of functions, and the processing of large and diverse workloads, results in a complexity and workload that make management control extremely difficult. It is because of this increased complexity and activity that an exception reporting process should be used as a diagnostic filter.

The concept of exception reporting is analogous to an automated medical system. By processing the monitored responses of a patient and matching them against previous patterns of illness and certain definable thresholds for blood pressure, blood counts, and other symptomatic conditions, it is possible to diagnose the illness.

The exception reporting system described in this chapter operates similarly. By using data from available monitoring sources (for example, RMF, CA TSO/MON PM, SMF) and comparing this activity against user-defined thresholds, the reporting process provides an integrated exception list that can help diagnose the data center's potential problem areas.

CA MICS exception reporting reduces the number and frequency of the reports that systems programmers, performance analysts, security officers, and other people have to interpret. Furthermore, reporting the exceptions from all the installed CA MICS products in an integrated manner reduces the time spent tracking problems, resulting in increasing the effectiveness of the systems and performance teams.

4.2 Exception Processing

Exception reporting provides management and technical personnel with a means to identify specific problems or problem areas, organize and report the problems in terms of their severity, integrate the problem reporting for all CA MICS products, and associate the problems with their respective management areas.

Figure 4-1 depicts the inputs, operational flow, and outputs related to this daily process.

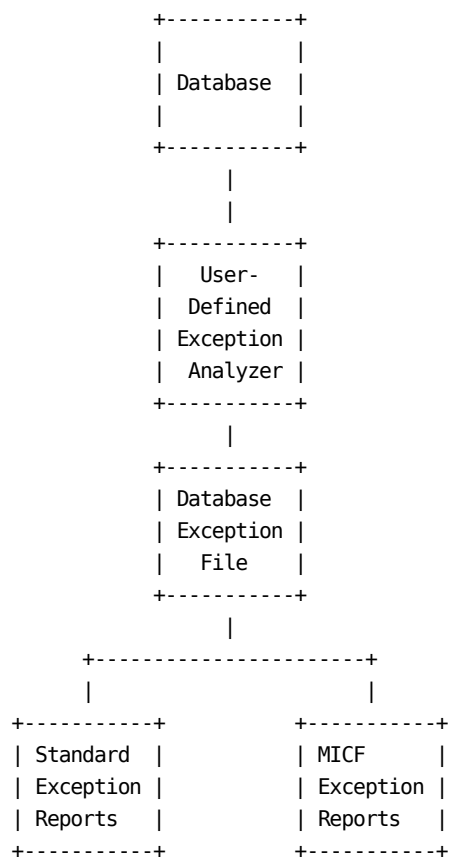


Figure 4-1. Exception Reporting Operational Flow

Each day, the updated database files are processed to detect the defined exception conditions. The exception analyzer performs this task by using test routines to identify the exceptions. Each test routine requires user-defined values to tailor the exception test to the installation.

requirements. The result of this processing is the Database Exception File, from which the standard and MICF reports are produced.

4.3 Using the Exception Reports for Problem Analysis

Standard reports and online inquiries are available for reporting the exception information. Using the reports effectively requires an understanding of the report structure.

First, CA MICS provides management with a concise summary of the frequency of problems in the exception management overview. An integrated, time-of-day oriented report (the severity level summary) provides the performance analyst and systems team with a summary of the exceptions, in the order of their severity, that have been detected for each hour of the day.

Based on the exceptions reported and the known problems, the performance analyst can then produce the Exception Full Detail Report by using MICF. This report can help the analyst assess quickly, and in greater depth, the DETAIL exceptions and the CA MICS database information from which they were detected to complete the research and resolution of the reported items.

4.4 Identification and Qualification

When a CA MICS product is developed, a set of exception conditions is defined to help management analyze the site's performance. Because the exceptions that CA MICS identifies are often voluminous, they require further qualifying so that the reports of exception items are organized and usable.

The exceptions that an installation can use are a standard part of CA MICS. The installation chooses the exceptions that it feels merit visibility and attention. This selection of pertinent exceptions is referred to as exception analysis. You may tailor the standard exceptions as explained in Chapter 2 of the Standard Reports Guide. CA MICS has a facility to assist you in determining the threshold values to use in the exceptions. This facility, the Exception Value Analysis process, is also explained in Chapter 2 of the Standard Reports Guide.

Each exception test may be identified within the source module by its assigned exception number. The test condition and its definition are written in SAS statements and consequently may be easily modified by the CA MICS System Administrator. The exception test condition also sets the exception number, defines the severity, assigns the exception to a management area, defines the appropriate text message to explain the exception, and establishes the necessary tests to identify the exception condition.

Each product's exception tests are identified and qualified in the following ways:

- o By exception number, for unique identification
- o By severity level, to signify degree of importance
- o By management area, to identify area of responsibility

The following sections discuss these topics:

- 1 - SNA Exception Number Assignment
- 2 - Severity Level Definition
- 3 - Management Area Definition

4.4.1 SNA Exception Number Assignment

Each exception test is assigned a unique reference number that enables you to refer to, analyze, and process the exception test. The number falls within the range of numbers assigned to the file whose data is being tested.

Figure 4-2 lists the range of exception numbers for the files in the CA MICS Network Analyzer Option.

Member Name	Descriptive Title
DYSNTEXC	Standard Exceptions
Exception Number Range	Database File Name
12001-12005	DETAIL.SNTNCL01
12061-12062	DETAIL.SNTCAF01
12121-12124	DETAIL.SNTNAF01
12154-12209	DETAIL.SNTNIN01
12301	DETAIL.SNTNSV01
12541-12542	DETAIL.SNTNEF01
12601	DETAIL.SNTNSF01
12661-12663	DETAIL.SNTPSU01
12780-12782	DETAIL.SNTNPL01
12801	DAYS.NVSLSY01
12802	DAYS.NVSNLL01
12852-12862	DAYS.NVSVBF01

Figure 4-2. SNT Exception Number Definition Table

4.4.2 Severity Level Definition

A severity level code is assigned to each exception. The assignment of the severity level enables the exception reports to emphasize the relative level of seriousness of the reported problems. It also provides a method for exception report selection.

The definition of severity level allows for three categories: critical, impacting, and warning. The assignment of severity level is, of course, subjective. The following guidelines are suggested for this purpose.

- o Critical. This is assigned to an exception that represents a missed service guarantee (e.g., availability, response, turnaround, etc.), a missed management objective (e.g., maximum of five IPLs per month), a security violation, or a serious violation of an installation standard or audit guideline.
- o Impacting. This is assigned to an exception that represents performance degradation related to reliability, service, capacity, turnaround, etc., that has created a political situation, or has in any way manifested itself in a noticeable problem short of the critical definition.
- o Warning. This is assigned to an exception that represents a preventive maintenance problem (e.g., buffers are running low), a symptomatic performance problem (e.g., demand paging rate is above normal), or a general installation standard or audit guideline that was violated.

4.4.3 Management Area Definition

The management area code is used primarily for reporting purposes and provides a means to organize the exceptions. A management area code is assigned to each exception and associates the exception with the relevant area of responsibility, for example, system availability. This code assignment enables the exceptions to be analyzed by a CA MICS information area or information area within management area.

The following list itemizes the management areas that are currently defined and in use:

- o Availability. This encompasses computing hardware (e.g., CPU) or software subsystems (e.g., TSO) reliability and availability.
- o Performance. Computing hardware, operations, supervisory software, or program product performance are included in this category.
- o Productivity. This area includes operational and development personnel productivity.
- o Security. This covers physical access, system integrity, and data access security.
- o Service. Online response times and batch turnarounds are included in this area.
- o Standards. The enforcement of installation-defined standards, guidelines, and policies make up the area of standards.
- o Workload. This refers to user-submitted load and the system effectiveness, performance, and operation.

4.5 CA MICS Network Standard Exceptions List

The exception selection routines are organized sequentially by exception number within the DYSNTEXC member and consist of SAS code. This code contains the exception selection criteria, severity level, management area, and the selection criteria for the exception test (e.g., selection of prime-time hours only). Each exception test condition has its name and number at the top so it can be located easily within the DYSNTEXC member. The value to be modified can then be changed directly within the SAS code.

The following table lists the standard exceptions provided with the CA MICS Network Analyzer Option, including the exception number, default severity level, management area code, and descriptive title.

Number	Severity	Management Area	Exception Description	Exception Source
12001	Impacting	Performance	Link Average Utilization Threshold Exceeded	NetSpy/NPM Network
12002	Impacting	Performance	Link Error Count Threshold Exceeded	NetSpy/NPM Network
12003	Impacting	Performance	Link Resource Outbound Queue Length Exceeded	NetSpy/NPM Network
12004	Impacting	Performance	Link Polling Rate Below Threshold	NetSpy/NPM Network
12005	Impacting	Performance	Link Positive Polling Percentage Threshold Exceeded	NetSpy/NPM Network
12061	Impacting	Performance	Network Component Error Threshold Exceeded	NetSpy/NPM Network
12062	Impacting	Performance	Component Resource Outbound Queue Length Exceeded	NetSpy/NPM Network
12121	Impacting	Performance	37XX CCU Utilization Above Limit	NetSpy/NPM Network
12122	Impacting	Performance	Percentage CCU Time in Slowdown Threshold Exceeded	NPM Network
12123	Impacting	Performance	Average Free Buffer Queue Length Below Limit	NetSpy/NPM Network
12124	Impacting	Performance	Avg NCP Channel Hold Queue Length Threshold Exceeded	NetSpy/NPM Network
12171	Impacting	Service	Host Response Time Exceeds Limit - for PLU/Line/SLU	NetSpy
12172	Impacting	Service	Network Response Time Exceeds Limit - for PLU/Line/SLU	NetSpy
12173	Impacting	Service	Total Response Time Exceeds Limit - for PLU/Line/SLU	NetSpy
12174	Impacting	Service	Worst Host Response Time Exceeds Limit	NetSpy
12175	Impacting	Service	Worst Network Response Time Exceeds Limit	NetSpy
12176	Impacting	Performance	Virtual Route Held/Blocked	NetSpy
12177	Warning	Performance	Number of Sessions for PLU Above Limit	NetSpy
12181	Warning	Performance	Network Component Traffic Exceeds Limit	NetSpy/NPM Network
12182	Critical	Performance	Network Component Traffic Below Minimum	NetSpy/NPM Network
12183	Critical	Performance	Network Component Error Rate Exceeds Limit	NetSpy/NPM Network
12184	Critical	Performance	37XX CCU Utilization Exceeds Limit	NetSpy/NPM Network
12185	Warning	Performance	37XX CCU Utilization Below Limit	NetSpy/NPM Network
12186	Impacting	Performance	Negative Poll Rate Exceeds Limit	NPM Network
12187	Impacting	Performance	Positive Poll Rate Below Limit	NPM Network
12188	Critical	Performance	Messages Per Minute Exceeds Limit	NetSpy/NPM Network
12189	Critical	Performance	Bytes Per Second Exceeds Limit	NetSpy/NPM Network
12190	Critical	Performance	Percentage of Free Buffers Below Minimum	NetSpy/NPM Network
12191	Critical	Performance	Outbound Queue Length Exceeds Limit	NetSpy/NPM Network
12192	Critical	Performance	Percentage of Time in Slowdown Exceeds Limit	NetSpy/NPM Network
12193	Impacting	Performance	Percentage of Bytes Retransmitted Exceeds Limit	NPM Network
12194	Critical	Performance	Percentage of NCP Buffers Used Exceeds Limit	NetSpy/NPM Network
12195	Warning	Performance	Percentage of NCP Buffers Used Below Limit	NetSpy/NPM Network
12196	Warning	Performance	Transmit Bytes Per Second Below Limit	NPM Network
12197	Critical	Performance	Transmit Bytes Per Second Exceeds Limit	NPM Network
12198	Warning	Performance	Receive Bytes Per Second Below Limit	NPM Network
12199	Critical	Performance	Receive Bytes Per Second Exceeds Limit	NPM Network
12200	Warning	Performance	Token Ring Interface % Utilization Below Limit	NPM Network
12201	Critical	Performance	Token Ring Interface % Utilization Exceeds Limit	NPM Network
12202	Warning	Performance	Congestion Count Below Limit	NPM Network
12203	Critical	Performance	Congestion Count Exceeds Limit	NPM Network

Figure 4-3. Network Exception List (Part 1 of 2)

Number	Severity	Management Area	Exception Description	Exception Source
12204	Warning	Performance	Percent Retransmitted Bytes Below Limit	NPM Network
12205	Critical	Performance	Percent Retransmitted Bytes Exceeds Limit	NPM Network
12206	Warning	Performance	Transmit PDU Per Minute Below Limit	NPM Network
12207	Critical	Performance	Transmit PDU Per Minute Exceeds Limit	NPM Network
12208	Warning	Performance	Receive PDU Per Minute Below Limit	NPM Network
12209	Critical	Performance	Receive PDU Per Minute Exceeds Limit	NPM Network
12541	Critical	Service	NPDA Event	NPDA or CA NetMaster
12542	Critical	Service	NPDA Event Alert	NPDA or CA NetMaster
12601	Critical	Service	NPDA Statistical Alert	NPDA or CA NetMaster
12661	Impacting	Service	Host Response Outside Bounds-Count Exceeded for SLU	NPM Session
12662	Impacting	Service	Net Response Outside Bounds-Count Exceeded for SLU	NPM Session
12663	Impacting	Service	Total Response Outside Bounds-Count Exceeded for SLU	NPM Session
12780	Impacting	Service	Host Response Outside Bounds-Count Exceeded for Link	NPM Session
12781	Impacting	Service	Net Response Outside Bounds-Count Exceeded for Link	NPM Session
12782	Impacting	Service	Total Response Outside Bounds-Count Exceeded for Link	NPM Session
12301	Impacting	Service	Response Objective Missed for Performance Class	NLDM or CA NetMaster
12801	Impacting	Service	Response Objective Missed for APPL/PCLASS	NLDM or CA NetMaster
12802	Impacting	Service	Response Objective Missed for LINK/PCLASS	NLDM or CA NetMaster
12852	Impacting	Service	Invalid Session Parameters Threshold Exceeded	NLDM or CA NetMaster
12853	Impacting	Service	Virtual Route Inoperative Threshold Exceeded	NLDM or CA NetMaster
12854	Impacting	Service	Route Extension Inoperative Threshold Exceeded	NLDM or CA NetMaster
12855	Impacting	Service	Hierarchical Reset Threshold Exceeded	NLDM or CA NetMaster
12856	Impacting	Service	SSCP Gone Threshold Exceeded	NLDM or CA NetMaster
12857	Impacting	Service	Virtual Route Deactivated Threshold Exceeded	NLDM or CA NetMaster
12858	Impacting	Service	LU Failure - Unrecoverable Threshold Exceeded	NLDM or CA NetMaster
12859	Impacting	Service	LU Failure - Recoverable Threshold Exceeded	NLDM or CA NetMaster
12862	Impacting	Service	Session Failure Threshold Exceeded	NLDM or CA NetMaster

Figure 4-4. Network Exception List (Part 2 of 2)

4.6 Detail Exception Descriptions

This section provides an in-depth description of each standard exception available in the exception report process. The exceptions are organized by number and appear sequentially starting with exception 12001.

The description format provides the title, number, and a statement on the purpose, rationale, and definition for each exception to give you some insight as to the meaning and use of the information. Finally, the SAS code is listed with a short explanation on how to modify the exception threshold values.

12001: Link Average Utilization Threshold Exceeded

FILE: NCP Link
SAS FILE NAME: DETAIL.SNTNCL01
SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
MANAGEMENT AREA: Performance (MGMTAREA='Performance')

PURPOSE: Identifies TP network links that have exceeded installation-defined thresholds.

RATIONALE: Network service to the end-user may degrade once certain levels of link utilization are attained.

This exception threshold should be set at a level that will indicate when link capacity limits are being reached. In general, these limits will differ for boundary links and links that make up transmission groups. Also the type of traffic being supported by the link may affect the threshold. For instance, links carrying RJE or BDT traffic can generally support higher utilization levels than links carrying interactive traffic.

DEFINITION: This exception condition is met when link utilization exceeds the installation-defined objective.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION, and are described below:

```
/* ***** */
/* EX NR: 12001 */
/* TITLE: LINK AVG UTIL THRESHOLD EXCEEDED */
/* FILE: DETAIL.SNTNCL01 */
/* ***** */

T_PCLBS=35; /* CHG THIS STATEMENT TO ADJUST THE THRESHOLD */
IF NCLPCLBS GT T_PCLBS THEN DO;
  ID = NETNAME;
  EXCCODE='12001'; SEVERITY='I'; MGMTAREA='SERVICE';
  EXCDDESC1=
    'LINK AVG UTILIZATION THRESHOLD EXCEEDED ' ;
  EXCDDESC2='AVERAGE LINK UTILIZATION= ' ||
    TRIM(PUT(NCLPCLBS,PERCENT.)) ||
    ', THRESHOLD= ' || TRIM(PUT(T_PCLBS,PERCENT.));
  LINK HIT;
END;
```

THRESHOLD MODIFICATION: Modify the value of T_PCLBS to represent the user-defined link utilization threshold.

12002: Link Error Count Threshold Exceeded

FILE: NCP Link
SAS FILE NAME: DETAIL.SNTNCL01
SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
MANAGEMENT AREA: Performance (MGMTAREA='Performance')

PURPOSE: Identifies CA NetSpy/NPM intervals during which the number of link errors exceeded site-defined levels.

RATIONALE: Both throughput and end-user response time are adversely affected by link errors and the resulting retransmission of data they cause. Typically, no links operate totally error-free over any macroscopic time period. All other things being equal, link error rates tend to increase with increasing link speed. Thus, the amount of data retransmitted when an error occurs must be adjusted, depending on the error rate of the link and the link speed. (Operands that affect the amount of data retransmitted are MAXDATA, MAXOUT, and PASSLIM of the PU macro and the RETRIES operand of the SDLCST macro).

Sudden significant increases in the link error rate may indicate a failing component on the link. Gradual increases in the link error rate may indicate that the NCP parameters for the link should be reevaluated.

DEFINITION: This exception condition is met when link error counts exceed site-defined thresholds.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12002 */
/* TITLE: LINK ERROR COUNT THRESHOLD EXCEEDED */
/* FILE: DETAIL.SNTNCL01 */
/* ***** */

T_NRERR=30; /* CHG THIS STATEMENT TO ADJUST THE THRESHOLD */
IF NCLNRERR GT T_NRERR THEN DO;
  ID =NETNAME;
  EXCCODE='12002'; SEVERITY='I'; MGMTAREA='PERFORMANCE';
  EXCDISC1='LINK ERROR COUNT THRESHOLD EXCEEDED ';
  EXCDISC2='LINK ERROR COUNT= ' ||
    TRIM(PUT(NCLNRERR,8.)) ||
    ', THRESHOLD= ' || TRIM(PUT(T_NRERR,8.));
  LINK HIT;
END;
```

THRESHOLD MODIFICATION: Modify the value of T_NRERR to represent the site-defined link error count threshold.

12003: Link Resource Outbound Queue Length Exceeded

FILE: NCP Link
SAS FILE NAME: DETAIL.SNTNCL01
SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
MANAGEMENT AREA: Performance (MGMTAREA='Performance')

PURPOSE: Identifies periods of excessive queuing of outbound messages in the communication controller.

RATIONALE: A large outbound queue length means that many messages from the host to the network are waiting to be sent. This condition quickly results in excessive network response times, and can cause NCP buffer congestion. This exception may occur with other exceptions to give a better indication of the real problem:

- o Processor or Messages Per Minute Overload -
Indicates a trend toward queue overloading due to high network processor CPU time. Examine line error rates and bytes-to-message ratios for possible improvements.
- o Bytes Per Second or Network Component (Line) Overload -
Indicates a trend toward queue overloading due to line saturation. This overuse may be general across all lines on the processor. If the overload is localized to a few lines, the line overload exception will appear. Examine the distribution of logical units (LUs) across lines for possible load distribution improvements.
- o Percentage of Time in Slowdown Exceeds Limit -
System definitions may cause NCP slowdown conditions. Examine network parameters, such as pacing, and other environmental descriptors, such as the Service Order Table, for possible improvements.
- o Free Buffer Percentage Below Limit -
The free buffer percentage exception indicates a processor loading trend which may lead to outbound queue length overloads. This situation may be caused by bursts of output from host teleprocessing monitors. Such bursts may result from operating system dispatching priority or job mix imbalances. Examine host areas for hardware, SCP, or teleprocessing monitor internal bottlenecks, such as:

- DASD device or channel contention
 - o High batch activity during peak TP hours
 - o CICS MAXTASK, SOS, or storage fragmentation
 - o CICS journal overloads
 - o IMS transaction scheduling contentions

DEFINITION: This exception is detected when the link outbound queue length exceeds the installation-defined threshold.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12003 */
/* TITLE: LINK RESOURCE OUTBOUND QUEUE LENGTH EXCEEDED */
/* FILE: DETAIL.SNTNCL01 */
/* ***** */
```

```
T_NRRQ=10; /* CHG THIS STATEMENT TO ADJUST THE THRESHOLD */
IF NCLNRRQ GT T_NRRQ THEN DO;
  ID = NETNAME;
  EXCCODE='12003'; SEVERITY='I'; MGMTAREA='PERFORMANCE';
  EXCDISC1='LINK RESOURCE OUTBOUND QUEUE LENGTH EXCEEDED ' ;
  EXCDISC2='OUTBOUND QUEUE LENGTH= ' ||
    TRIM(PUT(NCLNRRQ,8.)) ||
    ', THRESHOLD= ' || TRIM(PUT(T_NRRQ,8.));
  LINK HIT;
END;
```

THRESHOLD MODIFICATION: Modify the value of T_NRRQ to represent the installation-defined link outbound queue length threshold.

12004: Link Polling Rate Below Threshold

FILE: NCP Link
 SAS FILE NAME: DETAIL.SNTNCL01
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
 MANAGEMENT AREA: Performance (MGMTAREA='Performance')

PURPOSE: Detects periods of low polling on communication links.

RATIONALE: Interactive service levels are a function of the polling rate, since the cluster must be polled to initiate a transaction. The polling rate should be set based on the number of logical units (LUs) on the link and the amount of activity they generate.

A gradual reduction in the polling rate on a line may be due to an overall increase in CCU utilization; a sudden reduction is more likely due to a change in the NCP parameters.

Relevant NCP parameters are the PAUSE and POLIMIT operands of the LINE macro.

DEFINITION: This exception is detected when the link total polling rate falls below the installation-defined threshold.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12004 */
/* TITLE: LINK POLLING RATE BELOW THRESHOLD */
/* FILE: DETAIL.SNTNCL01 */
/* ***** */

T_PMTPL=20 ; /* CHG THIS STATEMENT TO ADJUST THE THRESHOLD */
IF NCLPMTPL LT T_PMTPL THEN DO;
  ID = NETNAME;
  EXCCODE='12004'; SEVERITY='I'; MGMTAREA='PERFORMANCE';
  EXCDISC1='LINK POLLING RATE BELOW THRESHOLD ' ;
  EXCDISC2='TOTAL POLLS= ' ||
    TRIM(PUT(NCLPMTPL,8.)) ||
    ', THRESHOLD= ' ||
    TRIM(PUT(T_PMTPL,8.)) ;
  LINK HIT;
END;
```

THRESHOLD MODIFICATION: Modify the value of T_PMTPL to represent the installation-defined link minimum total polling rate.

12005: Link Positive Polling Percentage Threshold Exceeded

FILE: NCP Link
 SAS FILE NAME: DETAIL.SNTNCL01
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects CA NetSpy/NPM measurement intervals during which a communication link's positive polling percentage was too high.

RATIONALE: A high positive polling percentage indicates that the majority of polls on the link are receiving a data response. This makes it likely that many transactions are waiting too long for a poll. An increase in the total polling rate would probably reduce end-user response time.

DEFINITION: This exception is detected when the link positive polling rate exceeds the site-defined threshold.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12005 */
/* TITLE: LINK POSITIVE POLLING PERCENTAGE EXCEEDS */
/* THRESHOLD */
/* FILE: DETAIL.SNTNCL01 */
/* ***** */

T_RTPPL=50; /* CHG THIS VARIABLE TO ADJUST THE THRESHOLD */
IF NCLNRTPPL GT ZERO THEN DO;
  NCLPCPPL=(NCLNRPPL/NCLNRTPPL)*100; /* TEMP FIELD */
  IF NCLPCPPL GT T_RTPPL THEN DO;
    ID = NETNAME;
    EXCCODE='12005'; SEVERITY='I'; MGMTAREA='PERFORMANCE';
    EXCDISC1=
      'LINK POSITIVE POLLING PERCENTAGE THRESHOLD EXCEEDED' ;
    EXCDISC2=
      'PERCENTAGE= ' || TRIM(PUT(NCLPCPPL,PERCENT.)) ||
      ', THRESHOLD= ' || TRIM(PUT(T_RTPPL,PERCENT.)) ;
    LINK HIT;
  END;
END;
```

THRESHOLD MODIFICATION: Modify the value of T_RTPPL to represent the user-defined link minimum positive polling rate.

12061: Network Component Error Threshold Exceeded

FILE: Network Components Activity
 SAS FILE NAME: DAYS.SNTCAF01
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects periods during which excessive temporary errors occurred for a network component.

RATIONALE: Temporary errors can be caused by several things, most of which have to do with the transmission line. Some temporary errors occur in all networks. Recognition of a trend toward increased temporary errors or error rates above a meaningful threshold can trigger preventive maintenance in time to prevent a hard failure. Temporary errors cost MCP CPU time in problem analysis and line time in retransmission.

DEFINITION: This exception is detected when a network component error count exceeds the installation-defined threshold.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12061 */
/* TITLE: NETWORK COMPONENT ERROR COUNT THRESHOLD EXCEEDED*/
/* FILE: DETAIL.SNTCAF01 */
/* ***** */
```

```
T_NRERR=155; /* CHG THIS VARIABLE TO ADJUST THE THRESHOLD */
IF CAFNRERR GT T_NRERR THEN DO;
  ID =NETNAME;
  EXCCODE='12061'; SEVERITY='I'; MGMTAREA='PERFORMANCE';
  EXCDISC1 =
    'NETWORK COMPONENT ERROR THRESHOLD EXCEEDED ' ;
  EXCDISC2= 'COMPONENT ERROR COUNT= ' ||
    TRIM(PUT(CAFNRERR,8.)) ||
    ', THRESHOLD= ' || TRIM(PUT(T_NRERR,8.));
  LINK HIT;
END;
```

THRESHOLD MODIFICATION: Modify the value of T_NRERR to represent the installation-defined network component error

rate threshold.

12062: Component Resource Outbound Queue Length Exceeded

FILE: Network Components Activity
 SAS FILE NAME: DAYS.SNTCAF01
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
 MANAGEMENT AREA: Performance (MGMTAREA='Performance')

PURPOSE: Identifies periods during which high communication controller message loading occurred due to network component queuing.

RATIONALE: A large outbound queue length means that many messages from the host to the network are waiting to be sent. This condition quickly results in overall host throughput degradation. This exception may occur with other exceptions to give a better indication of the real problem:

- o Processor or Messages Per Minute Overload -
 Indicates a trend toward queue overloading due to high network processor CPU time. Examine line error rates and bytes-to-message ratios for possible improvements.
- o Bytes Per Second or Network Component (Line) Overload -
 Indicates a trend toward queue overloading due to line saturation. This overuse may be general across all lines on the processor. If the overload is localized to a few lines, the line overload exception will appear. Examine the distribution of logical units (LUs) across lines for possible load distribution improvements.
- o Percentage of Time in Slowdown Exceeds Limit -
 System definitions may cause NCP slowdown conditions. Examine network parameters, such as pacing, and other environmental descriptors, such as the Service Order Table, for possible improvements.
- o Free Buffer Percentage Below Limit -
 The free buffer percentage exception indicates a processor loading trend which may lead to outbound queue length overloads. This situation may be caused by bursts of output from host teleprocessing monitors. Such bursts may result from operating system dispatching priority or job mix imbalances. Examine host areas for hardware, SCP, or teleprocessing monitor internal bottlenecks, such as:
 - DASD device or channel contention
 - High batch activity during peak TP hours

- CICS MAXTASK, SOS, or storage fragmentation
- CICS journal overloads
- IMS transaction scheduling contentions

DEFINITION: This exception is detected when the link outbound queue length exceeds the installation-defined threshold.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12062 */
/* TITLE: NETWORK COMPONENT OUTBOUND Q LENGTH EXCEEDED */
/* FILE: DETAIL.SNTCAF01 */
/* ***** */
```

```
T_NRRQ=70; /* CHG THIS VARIABLE TO ADJUST THE THRESHOLD */
IF CAFNRRQ GT T_NRRQ THEN DO;
  ID =NETNAME;
  EXCCODE='12062'; SEVERITY='I'; MGMTAREA='PERFORMANCE';
  EXCDISC1 =
    'COMPONENT RESOURCE OUTBOUND Q LENGTH EXCEEDED ' ;
  EXCDISC2= 'OUTBOUND QUEUE LENGTH= ' ||
    TRIM(PUT(CAFNRRQ,8.)) ||
    ', THRESHOLD= ' || TRIM(PUT(T_NRRQ,8.));
  LINK HIT;
END;
```

THRESHOLD MODIFICATION: Modify the value of T_NRRQ to represent the installation-defined network component outbound queue length threshold.

12121: 37XX CCU Utilization Above Limit

FILE: NCP Activity
 SAS FILE NAME: DETAIL.SNTNAF01;
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Identifies periods of high hardware cycle use in the communication controller.

RATIONALE: Overutilizing a 37XX processor can be caused by many environmental factors. Among these are having too many high-volume devices on a single processor and inappropriate distribution of the application work to be done. The CA MICS Network Analyzer can help identify these situations. This can aid the network administrator in reconfiguring the network to balance 37XX processors and can help user management balance application workload among available devices or plan for network expansion.

DEFINITION: This exception is detected when the 37XX utilization exceeds the installation-defined threshold.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12121 */
/* TITLE: 37XX CCU UTILIZATION ABOVE LIMIT */
/* EXCEEDED */
/* FILE: DETAIL.SNTNAF01 */
/* ***** */
```

```
T_PCCCU=90; /* CHG THIS VARIABLE TO ADJUST THE THRESHOLD */
IF NAFPPCCU GT T_PCCCU THEN DO;
  ID =NCPNAME;
  EXCCODE='12121'; SEVERITY='I'; MGMTAREA='PERFORMANCE';
  EXCDISC1 =
    '37XX CCU UTILIZATION ABOVE LIMIT' ;
  EXCDISC2= '37XX UTILIZATION= ' ||
    TRIM(PUT(NAFPCCCU,PERCENT.)) ||
    ', THRESHOLD= ' || TRIM(PUT(T_PCCCU,PERCENT.));
  LINK HIT;
END;
```

THRESHOLD MODIFICATION: Modify the value of T_PCCCU to represent the installation-defined 37xx utilization threshold.

12122: Percentage CCU Time in Slowdown Threshold Exceeded

FILE: NCP Activity
 SAS FILE NAME: DETAIL.SNTNAF01;
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Identifies CA NetSpy/NPM measurement intervals during which the communications controller was in slowdown (that is, buffer congestion).

RATIONALE: NCP slowdown is a symptom of insufficient memory in the 37xx processor. Slowdown occurs when the available buffer pool falls below the slowdown threshold that was set at 37xx generation. Slowdown degrades network performance because the 37xx attempts to send messages (thus freeing buffers) without receiving messages (which would consume buffers).

A fully utilized 37xx will experience some periods of slowdown, which should be considered normal. Excessive slowdown should be avoided because of the performance impact. If this occurs, examine network parameters, such as pacing, and other environmental descriptors, such as the Service Order Table, for possible improvements.

Networks that experience sudden fluctuations in traffic load may enter slowdown frequently even though the overall network utilization is low. Often this will occur when a certain application or group of network resources is activated. In this case, changes to the operational procedures can significantly improve performance, as the network may be operating in slowdown mode for considerable periods after the event that caused the slowdown has occurred.

DEFINITION: This exception is detected when the CCU slowdown threshold is exceeded.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12122 */
/* TITLE: PERCENTAGE CCU TIME IN SLOWDOWN THRESHOLD */
/* EXCEEDED */
```

```
/* FILE:  DETAIL.SNTNAF01                                */
/* ***** */

T_PCTIS=10; /* CHG THIS VARIABLE TO ADJUST THE THRESHOLD */
IF NAFPCTIS GT T_PCTIS THEN DO;
  ID =NCPNAME;
  EXCCODE='12122'; SEVERITY='I'; MGMTAREA='PERFORMANCE';
  EXCDDESC1 =
    'PCT CCU TIME IN SLOWDOWN THRESHOLD EXCEEDED ' ;
  EXCDDESC2= 'PERCENT TIME IN SLOWDOWN= ' ||
    TRIM(PUT(NAFPCTIS,PERCENT.)) ||
    ', THRESHOLD= ' || TRIM(PUT(T_PCTIS,PERCENT.));
  LINK HIT;
END;

THRESHOLD MODIFICATION:  Modify the value of T_PCTIS to
represent the site-defined 37xx time in slowdown threshold.
```

12123: Average Free Buffer Queue Length Below Limit

FILE: NCP Activity
 SAS FILE NAME: DETAIL.SNTNAF01;
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Identifies periods during which the 37xx average free buffer queue length fell below installation-defined objectives.

RATIONALE: A low percentage of free buffers indicates a trend toward some type of processor overload. This exception may occur with other exceptions to give a better indication of the real problem:

- o Processor or Messages Per Minute Overload -
 Indicates a trend toward queue overloading due to high network processor CPU time.
- o Bytes Per Second or Network Component (Line) Overload -
 Indicates a trend toward queue overloading due to line saturation. This overuse may be general across all lines on the processor. If the overload is localized to a few lines, the line overload exception will appear. Examine the distribution of logical units (LUs) across lines for possible load distribution improvements.
- o Percentage of Time in Slowdown Exceeds Limit -
 System definitions may cause NCP slowdown conditions. Examine network parameters, such as pacing, and other environmental descriptors, such as the Service Order Table, for possible improvements.
- o Outbound Queue Length Overload -
 The free buffer percentage exception indicates a processor loading trend which may lead to outbound queue length overloads. This situation may be caused by bursts of output from host teleprocessing monitors. Such bursts may result from operating system dispatching priority or job mix imbalances. Examine host areas for hardware, SCP, or teleprocessing monitor internal bottlenecks, such as:
 - DASD device or channel contention
 - High batch activity during peak TP hours
 - CICS MAXTASK, SOS, or storage fragmentation
 - CICS journal overloads

- IMS transaction scheduling contentions

DEFINITION: This exception is detected in CA MICS when the average free buffer queue length exceeds the installation-defined standards.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12123 */
/* TITLE: AVERAGE FREE BUFFER QUEUE LENGTH BELOW THRESHOLD*/
/* FILE: DETAIL.SNTNAF01 */
/* ***** */

T_AVFBQ=3400; /* CHG THIS VARIABLE TO ADJUST THE THRESHOLD */
IF NAFVFBQ LT T_AVFBQ THEN DO;
  ID =NCPNAME;
;
  EXCDISC2='AVG FREE BUFFER QUEUE LENGTH = ' ||
    TRIM(PUT(NAFVFBQ,8.)) ||
    ', THRESHOLD= ' || TRIM(PUT(T_AVFBQ,8.));
  LINK HIT;
END;
```

THRESHOLD MODIFICATION: Modify the value of T_AVFBQ to represent the installation-defined 37xx free buffer queue length threshold.

12124: Avg NCP Channel Hold Queue Length Threshold Exceeded

FILE: NCP Activity
 SAS FILE NAME: DETAIL.SNTNAF01;
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Identifies periods during which high communication controller inbound message queuing occurred due to insufficient service from one or more channel attached host processors.

RATIONALE: A large channel hold queue length indicates that messages are waiting to be sent from the network to the host. This condition is rare due to the high relative data transfer rate of the channel relative to communications lines. Occurrence of the exception generally indicates a channel problem exists or that the channel is improperly configured. Make certain that other devices sharing the channel with the 37xx are not monopolizing the channel.

DEFINITION: This exception is detected when the channel hold queue length exceeds the installation-defined threshold.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12124 */
/* TITLE: AVG NCP CHANNEL HOLD QUEUE LENGTH THRESHOLD */
/* EXCEEDED */
/* FILE: DETAIL.SNTNAF01 */
/* ***** */
```

```
T_AVHQL=8; /* CHG THIS VARIABLE TO ADJUST THE THRESHOLD */
IF NAFVHQL GT T_AVHQL THEN DO;
  ID =NCPNAME;
  EXCCODE='12124'; SEVERITY='I'; MGMTAREA='PERFORMANCE';
  EXCDDESC1 =
    'AVG NCP CHANNEL HOLD Q LENGTH THRESHOLD EXCEEDED ' ;
  EXCDDESC2= 'AVG CHANNEL HOLD Q LENGTH= ' ||
    TRIM(PUT(NAFVHQL,8.)) ||
    ', THRESHOLD= ' || TRIM(PUT(T_AVHQL,8.));
  LINK HIT;
END;
```

THRESHOLD MODIFICATION: Modify the value of T_AVHQL to define the user-defined 37xx hold channel queue length value.

12171: Host Response Time Exceeds Limit for PLU/LINE/SLU

FILE: Network Incident File
 SAS FILE NAME: DETAIL.SNTNIN01;
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
 MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies those CA NetSpy intervals during which end-user response time may have been poor due to host turnaround.

RATIONALE: End-user response time is divided into three categories by CA NetSpy:

- o Host response time - the amount of time required for the host hardware and software to service a request (or transaction). This includes VTAM time and host application time.
- o Network response time - the amount of time required for the network to service a request. This typically includes link transmission time, time in the control unit, and any time during which the request queued by the communications controller.
- o User response time - host plus network response time.

CA NetSpy allows you to specify high and low bounds for acceptable host response time. If actual response time falls outside those bounds, it creates a general alert.

DEFINITION: This exception is detected by the CA NetSpy general alert facility.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12171 */
/* TITLE: HOST RESPONSE TIME EXCEEDS LIMIT FOR */
/* PLU/LINE/SLU */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
IF NINCODE = 201 OR NINCODE = 1201
  THEN DO;
```

```
ID =NETNAME;
EXCCODE='12171'; SEVERITY='I'; MGMTAREA='SERVICE';
IF NINTYPE EQ 'E' THEN DO;
  EXCDDESC1 =
    'HOST RT EXCEEDS LIMIT, RESOURCE='
    || RESNAME || ',XRES=' || NINRESOL;
  EXCDDESC2='HI LIM=' || TRIM(LEFT(PUT(NINNRHIC,8.))) ||
    ',WAS=' || TRIM(LEFT(PUT(NINNRRVAL,8.)));
END;
ELSE DO;
  EXCDDESC1 =
    'HOST RT EXCEEDS LIMIT, RESOURCE='
    || RESNAME || ',REASON=' || NINEXCRC;
  EXCDDESC2='HI LIM=' || TRIM(LEFT(PUT(NINNRHIC,8.))) ||
    ',WAS=' || TRIM(LEFT(PUT(NINNRRVAL,8.))) ||
    ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
END;
LINK HIT;
END;
```

THRESHOLD MODIFICATION: Modify thresholds in the CA NetSpy ALERTPRM member.

12172: Net Response Time Exceeds Limit for PLU/LINE/SLU

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01;
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
 MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies those CA NetSpy intervals during which end-user response time may have been poor due to network service.

RATIONALE: End-user response time is divided into three categories by CA NetSpy:

- o Host response time - the amount of time required for the host hardware and software to service a request (or transaction). This includes VTAM time and host application time.
- o Network response time - the amount of time required for the network to service a request. This typically includes link transmission time, time in the control unit, and any time the request was queued by the communications controller.
- o User response time - host plus network response time.

CA NetSpy allows you to specify high and low bounds for acceptable network response time. If actual response time falls outside those bounds, it creates a general alert.

DEFINITION: This exception is detected by the CA NetSpy general alert facility.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12172 */
/* TITLE: NETWORK RESPONSE TIME EXCEEDS LIMIT FOR */
/* PLU/LINE/SLU */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
IF NINCODE = 203 OR NINCODE = 1203
THEN DO;
  ID =NETNAME;
```

```
EXCCODE='12172'; SEVERITY='I'; MGMTAREA='SERVICE';
IF NINTYPE EQ 'E' THEN DO;
  EXCDESC1 =
    'NETWORK RT EXCEEDS LIMIT, RESOURCE='
    || RESNAME || ',XRES=' || NINRESOL;
  EXCDESC2='HI LIM=' || TRIM(LEFT(PUT(NINNRHIC,8.))) ||
    ',WAS=' || TRIM(LEFT(PUT(NINNRRVAL,8.)));
END;
ELSE DO;
  EXCDESC1 =
    'NETWORK RT EXCEEDS LIMIT, RESOURCE='
    || RESNAME || ',REASON=' || NINEXCRC;
  EXCDESC2='HI LIM=' || TRIM(LEFT(PUT(NINNRHIC,8.))) ||
    ',WAS=' || TRIM(LEFT(PUT(NINNRRVAL,8.))) ||
    ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
  LINK HIT;
END;
```

THRESHOLD MODIFICATION: Modify thresholds in the CA NetSpy
ALERTPRM member.

12173: Total Response Time Exceeds Limit for PLU/LINE/SLU

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01;
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
 MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies those CA NetSpy intervals during which end-user total response time was poor.

RATIONALE: End-user response time is divided into three categories by CA NetSpy:

- o Host response time - the amount of time required for the host hardware and software to service a request (or transaction). This includes VTAM time and host application time.
- o Network response time - the amount of time required for the network to service a request. This typically includes link transmission time, time in the control unit, and any time during which the request is queued by the communications controller.
- o User response time - host plus network response time.

CA NetSpy allows you to specify high and low bounds for acceptable total response time. If actual response time falls outside those bounds, it creates a general alert.

DEFINITION: This exception is detected by the CA NetSpy general alert facility.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12173 */
/* TITLE: TOTAL RESPONSE TIME EXCEEDS LIMIT FOR */
/* PLU/LINE/SLU */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
IF NINCODE = 205 OR NINCODE = 1205
THEN DO;
  ID =NETNAME;
```

```
EXCCODE='12173'; SEVERITY='I'; MGMTAREA='SERVICE';
IF NINTYPE EQ 'E' THEN DO;
  EXCDESC1 =
    'TOTAL RT EXCEEDS LIMIT, RESOURCE='
    || RESNAME || ',XRES=' || NINRESOL;
  EXCDESC2='HI LIM=' || TRIM(LEFT(PUT(NINNRHIC,8.))) ||
    ',WAS=' || TRIM(LEFT(PUT(NINNRVAL,8.)));
END;
ELSE DO;
  EXCDESC1 =
    'TOTAL RT EXCEEDS LIMIT, RESOURCE='
    || RESNAME || ',REASON=' || NINEXCRC;
  EXCDESC2='HI LIM=' || TRIM(LEFT(PUT(NINNRHIC,8.))) ||
    ',WAS=' || TRIM(LEFT(PUT(NINNRVAL,8.))) ||
    ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
END;
LINK HIT;
END;
```

THRESHOLD MODIFICATION: Modify thresholds in the CA NetSpy
ALERTPRM member.

12174: Worst Host Resp Time Exceeds Limit

FILE: Network Incident File
 SAS FILE NAME: DETAIL.SNTNIN01;
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
 MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies those CA NetSpy intervals during which end-user response time may have been poor due to host turnaround.

RATIONALE: End-user response time is divided into three categories by CA NetSpy:

- o Host response time - the amount of time required for the host hardware and software to service a request (or transaction). This includes VTAM time and host application time.
- o Network response time - the amount of time required for the network to service a request. This typically includes link transmission time, time in the control unit, and any time during which the request queued by the communications controller.
- o User response time - host plus network response time.

CA NetSpy allows you to specify high and low bounds for worst host response time. If actual response time falls outside those bounds, it creates a general alert.

DEFINITION: This exception is detected by the CA NetSpy general alert facility.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12174 */
/* TITLE: WORST HOST RESPONSE TIME EXCEEDS LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
IF NINCODE = 207 OR NINCODE = 1207
  THEN DO;
    ID =NETNAME;
```

```
EXCCODE='12174'; SEVERITY='I'; MGMTAREA='SERVICE';
IF NINTYPE EQ 'E' THEN DO;
  EXCDESC1 =
    'WORST HOST RT EXCEEDS LIMIT, RESOURCE='
    || RESNAME || ',XRES=' || NINRESOL;
  EXCDESC2='HI LIM=' || TRIM(LEFT(PUT(NINNRHIC,8.))) ||
    ',WAS=' || TRIM(LEFT(PUT(NINNRVAL,8.)));
END;
ELSE DO;
  EXCDESC1 =
    'WORST HOST RT EXCEEDS LIMIT, RESOURCE='
    || RESNAME || ',REASON=' || NINEXCRC;
  EXCDESC2='HI LIM=' || TRIM(LEFT(PUT(NINNRHIC,8.))) ||
    ',WAS=' || TRIM(LEFT(PUT(NINNRVAL,8.))) ||
    ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
END;
LINK HIT;
END;
```

THRESHOLD MODIFICATION: Modify thresholds in the CA NetSpy
ALERTPRM member.

12175: Worst Network Response Time Exceeds Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01;
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
 MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies those CA NetSpy measurement intervals during which end-user response time may have been poor due to network service.

RATIONALE: End-user response time is divided into three categories by CA NetSpy:

- o Host response time - the amount of time required for the host hardware and software to service a request (or transaction). This includes VTAM time and host application time.
- o Network response time - the amount of time required for the network to service a request. This typically includes link transmission time, time in the control unit, and any time the request was queued by the communications controller.
- o User response time - host plus network response time.

CA NetSpy allows you to specify high and low bounds for the worst network response time. If actual response time falls outside those bounds, it creates a general alert.

DEFINITION: This exception is detected by the CA NetSpy general alert facility.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12175 */
/* TITLE: WORST NETWORK RESPONSE TIME EXCEEDS LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
IF NINCODE = 209 OR NINCODE = 1209
THEN DO;
  ID =NETNAME;
  EXCCODE='12175'; SEVERITY='I'; MGMTAREA='SERVICE';
```

```
IF NINTYPE EQ 'E' THEN DO;
  EXCDESC1 =
    'WORST NET RT EXCEEDS LIMIT, RESOURCE='
    || RESNAME || ',XRES=' || NINRESOL;
  EXCDESC2='HI LIM=' || TRIM(LEFT(PUT(NINNRHIC,8.))) ||
    ',WAS=' || TRIM(LEFT(PUT(NINNRVAL,8.)));
END;
ELSE DO;
  EXCDESC1 =
    'WORST NET RT EXCEEDS LIMIT, RESOURCE='
    || RESNAME || ',REASON=' || NINEXCRC;
  EXCDESC2='HI LIM=' || TRIM(LEFT(PUT(NINNRHIC,8.))) ||
    ',WAS=' || TRIM(LEFT(PUT(NINNRVAL,8.))) ||
    ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
END;
LINK HIT;
END;
```

THRESHOLD MODIFICATION: Modify thresholds in the CA NetSpy
ALERTPRM member.

12176: Virtual Route Held/Blocked

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01;
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
 MANAGEMENT AREA: Service (MGMTAREA='PERFORMANCE')

PURPOSE: Identifies those CA NetSpy intervals during which a virtual route (logical network path) is congested.

RATIONALE: A virtual route has three possible active states: open (normal), held (moderately congested), and blocked (severely congested). Blocked and held VRs degrade response time and throughput for all sessions traversing the route.

DEFINITION: This exception is detected by the CA NetSpy general alert facility.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```

/* ***** */
/* EX NR: 12176 */
/* TITLE: VIRTUAL ROUTE HELD/BLOCKED */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
IF NINCODE = 251 OR NINCODE = 1251
THEN DO;
  ID =NETNAME;
  EXCCODE='12176'; SEVERITY='I'; MGMTAREA='PERFORMANCE';
  IF NINTYPE EQ 'E' THEN DO;
    EXCDDESC1 =
      'VIRTUAL ROUTE HELD/BLOCKED, RESOURCE='
      || RESNAME || ',XRES=' || NINRESOL;
    EXCDDESC2='HI LIM=' || TRIM(LEFT(PUT(NINNRHIC,8.))) ||
      ',WAS(% TIME IN SEC)= ' || TRIM(LEFT(PUT(NINNRVAL,8.)));
  END;
ELSE DO;
  'VIRTUAL ROUTE HELD/BLOCKED, RESOURCE='
  || RESNAME || ',REASON=' || NINEXCRC;
  EXCDDESC2='HI LIM=' || TRIM(LEFT(PUT(NINNRHIC,8.))) ||
    ',WAS(% TIME IN SEC)= ' || TRIM(LEFT(PUT(NINNRVAL,8.))) ||
    ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
END;

```

LINK HIT;
END;

THRESHOLD MODIFICATION: Modify thresholds in the CA NetSpy
ALERTPRM member.

12177: Number of Sessions for PLU Exceeds Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01;
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Warning (SEVERITY='W')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Identifies those CA NetSpy intervals during which the number of users logged on to a PLU (application) exceeded the alert threshold limit defined to CA NetSpy.

RATIONALE: Host response time for an application can become degraded if an excessive number of users are logged on concurrently.

DEFINITION: This exception is detected by the CA NetSpy general alert facility.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12177 */
/* TITLE: NUMBER OF SESSIONS FOR PLU ABOVE LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
IF NINCODE = 241 OR NINCODE = 1241
THEN DO;
  ID =NETNAME;
  EXCCODE='12177'; SEVERITY='W'; MGMTAREA='PERFORMANCE';
  IF NINTYPE EQ 'E' THEN DO;
    EXCDDESC1 =
      'NUMBER OF SESSIONS FOR PLU ABOVE LIMIT, RESOURCE='
      || RESNAME || ',XRES=' || NINRESOL;
    EXCDDESC2='HI LIM=' || TRIM(LEFT(PUT(NINNRHIC,8.))) ||
      ',WAS=' || TRIM(LEFT(PUT(NINNRVAL,8.)));
  END;
ELSE DO;
  EXCDDESC1 =
    'NUMBER OF SESSIONS FOR PLU ABOVE LIMIT, RESOURCE='
    || RESNAME || ',REASON=' || NINEXCRC;
  EXCDDESC2='HI LIM=' || TRIM(LEFT(PUT(NINNRHIC,8.))) ||
    ',WAS=' || TRIM(LEFT(PUT(NINNRVAL,8.))) ||
    ',INTV=' || TRIM(LEFT(PUT(NINNREXI,3.)));
END;
```

```
END;  
LINK HIT;  
END;
```

THRESHOLD MODIFICATION: Modify thresholds in the CA NetSpy
ALERTPRM member.

12181: Network Component Traffic Exceeds Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Critical (SEVERITY='C')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects an overutilized network component.

RATIONALE: Overutilization of a network component can be caused by many environmental factors. Among these are, having too few devices to handle typical or peak application workloads and inappropriately distributing the application work to be done. The CA MICS Network Analyzer Option can help identify these situations. This can aid the network administrator in reconfiguring the network to balance controllers and lines. This can also help user management balance application workload among available devices or plan for network expansion.

DEFINITION: This exception is detected by either the CA NetSpy general alert facility or the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12181 */
/* TITLE: NETWORK COMPONENT TRAFFIC EXCEEDS LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
IF NINCODE = 001 OR NINCODE = 1001
THEN DO;
  ID =NETNAME;
  EXCCODE='12181'; SEVERITY='C'; MGMTAREA='PERFORMANCE';
  IF NINTYPE EQ 'E' THEN DO;
    EXCDISC1 =
      'NETWORK COMPONENT TRAFFIC EXCEEDS LIMIT ' ||
      ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
    EXCDISC2= 'HI LIM=' || TRIM(PUT(NINNRHIC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRVAL,8.));
  END;
ELSE DO;
  EXCDISC1 =
```

```
'NETWORK COMPONENT TRAFFIC EXCEEDS LIMIT ' ||  
' ,NCP=' || NCPNAME || ' ,REASON=' || NINEXCRC;  
EXCDESC2= 'HI LIM=' || TRIM(PUT(NINNRHIC,8.)) ||  
          ' ,WAS=' || TRIM(PUT(NINNRVAL,8.)) ||  
          ' ,INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));  
  
END;  
LINK HIT;  
END;
```

THRESHOLD MODIFICATION: Modify thresholds in the CA NetSpy
ALERTPRM member or in the NPM START MONITOR command.

12182: Network Component Traffic Below Minimum

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Warning (SEVERITY='W')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects an underutilized network component.

RATIONALE: Underutilizing a network component can be caused by many environmental factors. Among these are having too many devices to handle typical or peak application workloads and inappropriately distributing the application work to be done. The CA MICS Network Analyzer Option can help identify these situations. This can aid the network administrator in reconfiguring the network to balance controllers and lines. This can also help user management balance application workload among available devices, or plan for network expansion.

DEFINITION: This exception is detected by either the CA NetSpy general alert facility or the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12182 */
/* TITLE: NETWORK COMPONENT TRAFFIC BELOW MINIMUM */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
IF NINCODE = 002 OR NINCODE = 1002
THEN DO;
  ID =NETNAME;
  EXCCODE='12182'; SEVERITY='W'; MGMTAREA='PERFORMANCE';
  IF NINTYPE EQ 'E' THEN DO;
    EXCDISC1 =
      'NETWORK COMPONENT TRAFFIC BELOW MINIMUM' ||
      ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
    EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRLVAL,8.));
  END;
ELSE DO;
  EXCDISC1 =
    'NETWORK COMPONENT TRAFFIC BELOW MINIMUM' ||
```

```
      ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;  
      EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||  
                ',WAS=' || TRIM(PUT(NINNRLV,8.)) ||  
                ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));  
      END;  
      LINK HIT;  
      END;
```

THRESHOLD MODIFICATION: Modify thresholds in the CA NetSpy
ALERTPRM member or in the NPM START MONITOR command.

12183: Network Component Traffic Below Minimum

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Warning (SEVERITY='W')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects an underutilized network component.

RATIONALE: Underutilization of a network component can be caused by many environmental factors. Among these are having too many devices to handle typical or peak application workloads and inappropriately distributing the application work to be done. The CA MICS Network Analyzer Option can help identify these situations. This can aid the network administrator in reconfiguring the network to balance controllers and lines. This can also help user management balance application workload among available devices, or plan for network expansion.

DEFINITION: This exception is detected by either the CA NetSpy general alert facility or the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```

/* ***** */
/* EX NR: 12183 */
/* TITLE: NETWORK COMPONENT ERROR RATE EXCEEDS LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
IF NINCODE = 003 OR NINCODE = 1003
THEN DO;
  ID =NETNAME;
  EXCCODE='12183'; SEVERITY='C'; MGMTAREA='PERFORMANCE';
  IF NINTYPE EQ 'E' THEN DO;
    EXCDDESC1 =
      'NETWORK COMPONENT ERROR RATE EXCEEDS LIMIT' ||
      ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
    EXCDDESC2= 'HI LIM=' || TRIM(PUT(NINNRHIC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRVAL,8.));
  END;
ELSE DO;
  EXCDDESC1 =
    'NETWORK COMPONENT ERROR RATE EXCEEDS LIMIT' ||

```

```
' ,NCP=' || NCPNAME || ' ,REASON=' || NINEXCRC;  
EXCDESC2= 'HI LIM=' || TRIM(PUT(NINNRHIC,8.)) ||  
          ' ,WAS=' || TRIM(PUT(NINNRVAL,8.)) ||  
          ' ,INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));  
  
END;  
LINK HIT;  
END;
```

THRESHOLD MODIFICATION: Modify thresholds in the CA NetSpy
ALERTPRM member or in the NPM START MONITOR command.

12184: 37XX CCU Utilization Above Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Critical (SEVERITY='C')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects an overutilized 37XX processor.

RATIONALE: Overutilization of a 37XX processor can be caused by many environmental factors. Among these are having too many high-volume devices on a single processor and inappropriately distributing the application work to be done. The CA MICS Network Analyzer Option can help identify these situations. This can aid the network administrator in reconfiguring the network to balance 37XX processors. This can also help user management balance application workload among available devices or plan for network expansion.

DEFINITION: This exception is detected by either the CA NetSpy general alert facility or the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```

/* ***** */
/* EX NR: 12184 */
/* TITLE: 37XX CCU UTILIZATION ABOVE LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
IF NINCODE = 101 OR NINCODE = 1101
THEN DO;
  ID =NETNAME;
  EXCCODE='12184'; SEVERITY='C'; MGMTAREA='PERFORMANCE';
  IF NINTYPE EQ 'E' THEN DO;
    EXCDDESC1 =
      '37XX CCU UTILIZATION ABOVE LIMIT' ||
      ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
    EXCDDESC2= 'HI LIM=' || TRIM(PUT(NINNRRHC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRRVAL,8.));
  END;
ELSE DO;
  EXCDDESC1 =
    '37XX CCU UTILIZATION ABOVE LIMIT' ||
    ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;

```

```
EXCDESC2= 'HI LIM=' || TRIM(PUT(NINNRHIC,8.)) ||  
          ',WAS=' || TRIM(PUT(NINNRVAL,8.)) ||  
          ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));  
END;  
LINK HIT;  
END;
```

THRESHOLD MODIFICATION: Modify thresholds in the CA NetSpy
ALERTPRM member or in the NPM START MONITOR command.

12185: 37XX CCU Utilization Below Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Warning (SEVERITY='W')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects an underutilized 37XX processor.

RATIONALE: Underutilization of a 37XX processor can be caused by many environmental factors. Among these are having too few devices to generate a substantial workload and inappropriately distributing the application work to be done. The CA MICS Network Analyzer Option can help identify these situations and can aid the network administrator in reconfiguring the network to balance 37XX processors. This can also help user management balance application workload among available devices or plan for network expansion.

DEFINITION: This exception is detected by either the CA NetSpy general alert facility or the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```

/* ***** */
/* EX NR: 12185 */
/* TITLE: 37XX CCU UTILIZATION BELOW LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
IF NINCODE = 102 OR NINCODE = 1102
THEN DO;
  ID =NETNAME;
  EXCCODE='12185'; SEVERITY='W'; MGMTAREA='PERFORMANCE';
  IF NINTYPE EQ 'E' THEN DO;
    EXCDISC1 =
      '37XX CCU UNDERUTILIZED' ||
      ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
    EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRLVAL,8.));
  END;
ELSE DO;
  EXCDISC1 =
    '37XX CCU UNDERUTILIZED' ||
    ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;

```

```
EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||  
          ',WAS=' || TRIM(PUT(NINNRLV,8.)) ||  
          ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));  
END;  
LINK HIT;  
END;
```

THRESHOLD MODIFICATION: Modify thresholds in the CA NetSpy
ALERTPRM member or in the NPM START MONITOR command.

12186: Negative Poll Rate Exceeds Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects an unexpectedly high negative poll rate.

RATIONALE: A high negative polling rate indicates an excessive (unnecessarily high) polling rate. Reducing the polling rate for such components can reduce 37XX utilization and allow more components to be serviced from the same processor.

DEFINITION: This exception is detected through the NPM monitor exception records.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```

/* ***** */
/* EX NR: 12186 */
/* TITLE: NEGATIVE POLL RATE EXCEEDS LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
IF NINCODE = 103 OR NINCODE = 1103
THEN DO;
  ID =NETNAME;
  EXCCODE='12186'; SEVERITY='I'; MGMTAREA='PERFORMANCE';
  IF NINTYPE EQ 'E' THEN DO;
    EXCDDESC1 =
      'NEGATIVE POLL RATE EXCEEDS LIMIT' ||
      ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
    EXCDDESC2= 'HI LIM=' || TRIM(PUT(NINNRHIC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRRVAL,8.));
  END;
ELSE DO;
  EXCDDESC1 =
    'NEGATIVE POLL RATE EXCEEDS LIMIT' ||
    ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
    EXCDDESC2= 'HI LIM=' || TRIM(PUT(NINNRHIC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRRVAL,8.)) ||
      ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
  END;
END;

```

LINK HIT;
END;

THRESHOLD MODIFICATION: Perform threshold modification in the CRITERIA operand of the NPM START MONITOR command.

12187: Positive Poll Rate Below Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects an unexpectedly low positive poll rate.

RATIONALE: A low positive polling rate indicates an excessive (unnecessarily high) polling rate. Reducing the polling rate for such components can reduce 37XX utilization and allow more components to be serviced from the same processor.

DEFINITION: This exception is detected through the NPM monitor exception records.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```

/* ***** */
/* EX NR: 12187 */
/* TITLE: POSITIVE POLL RATE BELOW LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
IF NINCODE = 104 OR NINCODE = 1104
THEN DO;
  ID =NETNAME;
  EXCCODE='12187'; SEVERITY='I'; MGMTAREA='PERFORMANCE';
  IF NINTYPE EQ 'E' THEN DO;
    EXCDISC1 =
      'POSITIVE POLL RATE BELOW LIMIT' ||
      ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
    EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRLV,8.));
  END;
ELSE DO;
  EXCDISC1 =
    'POSITIVE POLL RATE BELOW LIMIT' ||
    ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
    EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRLV,8.)) ||
      ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
  END;
END;
```

LINK HIT;
END;

THRESHOLD MODIFICATION: Perform threshold modification in the CRITERIA operand of the NPM START MONITOR command.

12188: Messages Per Minute Exceeds Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Critical (SEVERITY='C')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects a high message volume.

RATIONALE: Each message processed by the network control program causes a certain amount of overhead. This overhead can be balanced to message size to keep the processor optimally busy without overloading. High message volume typically results in premature processor CPU saturation. Exceptions of this type may be accompanied by processor overload or bytes per second overload exceptions. If this is the case, the processor is merely overloaded. If the bytes per second exception does not occur, the processor overload may occur because of the number of messages processed. This exception appearing without the other two indicates a trend toward processor overload. Examine applications for possible repackaging of messages for a more efficient (higher) ratio of bytes to messages.

DEFINITION: This exception is detected by either the CA NetSpy general alert facility or the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12188 */
/* TITLE: MESSAGES PER MINUTE EXCEEDS LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
IF NINCODE = 105 OR NINCODE = 1105
THEN DO;
  ID =NETNAME;
  EXCCODE='12188'; SEVERITY='C'; MGMTAREA='PERFORMANCE';
  IF NINTYPE EQ 'E' THEN DO;
    EXCDISC1 =
      'MESSAGES PER MINUTE EXCEEDS LIMIT' ||
      ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
    EXCDISC2= 'HI LIM=' || TRIM(PUT(NINNRHIC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRVAL,8.));
```

```
END;  
ELSE DO;  
  EXCDESC1 =  
    'MESSAGES PER MINUTE EXCEEDS LIMIT' ||  
    ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;  
  EXCDESC2= 'HI LIM=' || TRIM(PUT(NINNRHIC,8.)) ||  
    ',WAS=' || TRIM(PUT(NINNRRVAL,8.)) ||  
    ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));  
END;  
LINK HIT;  
END;
```

THRESHOLD MODIFICATION: Modify thresholds in the CA NetSpy
ALERTPRM member or in the NPM START MONITOR command.

12189: Bytes Per Second Exceeds Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Critical (SEVERITY='C')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects a high character transmission volume.

RATIONALE: Each message processed by the network control program causes a certain amount of overhead. This overhead can be balanced to message size to keep the processor optimally busy without overloading. A high volume of characters transmitted typically results in premature processor output saturation. Exceptions of this type may be accompanied by processor overload or messages per minute overload exceptions. If this is the case, the processor is merely overloaded. If the messages per minute exception does not occur, the processor overload may occur because of the number of bytes processed. This exception appearing without the other two indicates a trend toward processor output overload. Examine applications for possible repackaging of messages for a more efficient (lower) ratio of bytes to messages, and the distribution of high character volume devices among processors.

DEFINITION: This exception is detected by either the CA NetSpy general alert facility or the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12189 */
/* TITLE: BYTES PER SECOND EXCEEDS LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
IF NINCODE = 106 OR NINCODE = 1106
THEN DO;
  ID =NETNAME;
  EXCCODE='12189'; SEVERITY='C'; MGMTAREA='PERFORMANCE';
  IF NINTYPE EQ 'E' THEN DO;
    EXCDDESC1 =
      'BYTES PER SECOND EXCEEDS LIMIT' ||
      ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
```

```
EXCDESC2= 'HI LIM=' || TRIM(PUT(NINNRHIC,8.)) ||  
          ',WAS=' || TRIM(PUT(NINNRVAL,8.));  
END;  
ELSE DO;  
EXCDESC1 =  
  'BYTES PER SECOND EXCEEDS LIMIT' ||  
  ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;  
EXCDESC2= 'HI LIM=' || TRIM(PUT(NINNRHIC,8.)) ||  
          ',WAS=' || TRIM(PUT(NINNRVAL,8.)) ||  
          ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));  
END;  
LINK HIT;  
END;
```

THRESHOLD MODIFICATION: Modify thresholds in the CA NetSpy
ALERTPRM member or in the NPM START MONITOR command.

12190: Percentage of Free Buffers Below Minimum

FILE: Network Incident
SAS FILE NAME: DETAIL.SNTNIN01
SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Critical (SEVERITY='C')
MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects high processor message loading.

RATIONALE: A low percentage of free buffers indicates a trend toward some type of processor overload. This exception may occur with other exceptions to give a better indication of the real problem:

- o Processor or Messages Per Minute Overload -
Indicates a trend toward queue overloading due to high network processor CPU time.
- o Bytes Per Second or Network Component (Line) Overload -
Indicates a trend toward queue overloading due to line saturation. This overuse may be general across all lines on the processor. If the overload is localized to a few lines, the line overload exception will appear. Examine the distribution of logical units (LUs) across lines for possible load distribution improvements.
- o Percentage of Time in Slowdown Exceeds Limit -
System definitions may cause NCP slowdown conditions. Examine network parameters, such as pacing, and other environmental descriptors, such as the service order table, for possible improvements.
- o Outbound Queue Length Overload -
The free buffer percentage exception indicates a processor loading trend which may lead to outbound queue length overloads. This situation may be caused by bursts of output from host teleprocessing monitors. Such bursts may result from operating system dispatching priority or job mix imbalances. Examine host areas for hardware, SCP, or teleprocessing monitor internal bottlenecks, such as:
 - DASD device or channel contention
 - High batch activity during peak TP hours
 - CICS MAXTASK, SOS, or storage fragmentation
 - CICS journal overloads
 - IMS transaction scheduling contentions

DEFINITION: This exception is detected by either the CA NetSpy general alert facility or the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12190 */
/* TITLE: PERCENTAGE OF FREE BUFFERS BELOW MINIMUM */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
IF NINCODE = 107 OR NINCODE = 1107
THEN DO;
  ID =NETNAME;
  EXCCODE='12190'; SEVERITY='C'; MGMTAREA='PERFORMANCE';
  IF NINTYPE EQ 'E' THEN DO;
    EXCDDESC1 =
      'PERCENTAGE OF FREE BUFFERS BELOW MINIMUM' ||
      ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
    EXCDDESC2= 'LOW LIM=' || TRIM(PUT(NINNRLLOC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRRVAL,8.));
  END;
ELSE DO;
  EXCDDESC1 =
    'PERCENTAGE OF FREE BUFFERS BELOW MINIMUM' ||
    ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
  EXCDDESC2= 'LOW LIM=' || TRIM(PUT(NINNRLLOC,8.)) ||
    ',WAS=' || TRIM(PUT(NINNRRVAL,8.)) ||
    ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
END;
LINK HIT;
END;
```

THRESHOLD MODIFICATION: Modify thresholds in the CA NetSpy ALERTPRM member or in the NPM START MONITOR command.

12191: Outbound Queue Length Exceeds Limit

FILE: Network Incident
SAS FILE NAME: DETAIL.SNTNIN01
SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Critical (SEVERITY='C')
MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects high processor message loading.

RATIONALE: A large outbound queue length means that many messages from the host to the network are waiting to be sent. This condition quickly results in overall host throughput degradation. This exception may occur with other exceptions to give a better indication of the real problem:

- o Processor or Messages Per Minute Overload -
Indicates a trend toward queue overloading due to high network processor CPU time. Examine line error rates and bytes-to-message ratios for possible improvements.
- o Bytes Per Second or Network Component (Line) Overload -
Indicates a trend toward queue overloading due to line saturation. This overuse may be general across all lines on the processor. If the overload is localized to a few lines, the line overload exception will appear. Examine the distribution of logical units (LUs) across lines for possible load distribution improvements.
- o Percentage of Time in Slowdown Exceeds Limit -
System definitions may cause NCP slowdown conditions. Examine network parameters, such as pacing, and other environmental descriptors, such as the Service Order Table, for possible improvements.
- o Free Buffer Percentage Below Limit -
The free buffer percentage exception indicates a processor loading trend which may lead to outbound queue length overloads. This situation may be caused by bursts of output from host teleprocessing monitors. Such bursts may result from operating system dispatching priority or job mix imbalances. Examine host areas for hardware, SCP, or teleprocessing monitor internal bottlenecks, such as:
 - DASD device or channel contention
 - High batch activity during peak TP hours
 - CICS MAXTASK, SOS, or storage fragmentation

- CICS journal overloads
- IMS transaction scheduling contentions

DEFINITION: This exception is detected by either the CA NetSpy general alert facility or the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12191 */
/* TITLE: OUTBOUND QUEUE LENGTH OVERLOAD */
/* FILE:  DETAIL.SNTNIN01 */
/* ***** */
IF NINCODE = 108 OR NINCODE = 1108
THEN DO;
  ID =NETNAME;
  EXCCODE='12191'; SEVERITY='C'; MGMTAREA='PERFORMANCE';
  IF NINTYPE EQ 'E' THEN DO;
    EXCDDESC1 =
      'OUTBOUND QUEUE LENGTH OVERLOAD' ||
      ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
    EXCDDESC2= 'HI LIM=' || TRIM(PUT(NINNRHIC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRRVAL,8.));
  END;
ELSE DO;
  EXCDDESC1 =
    'OUTBOUND QUEUE LENGTH OVERLOAD' ||
    ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
  EXCDDESC2= 'HI LIM=' || TRIM(PUT(NINNRHIC,8.)) ||
    ',WAS=' || TRIM(PUT(NINNRRVAL,8.)) ||
    ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
END;
LINK HIT;
END;
```

THRESHOLD MODIFICATION: Modify thresholds in the CA NetSpy ALERTPRM member or in the NPM START MONITOR command.

12192: Percentage of Time in Slowdown Exceeds Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Critical (SEVERITY='C')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects an NCP slowdown condition.

RATIONALE: System definitions may cause NCP slowdown conditions. Examine network parameters, such as pacing, and other environmental descriptors, such as the service order table, for possible improvements.

DEFINITION: This exception is detected by either the CA NetSpy general alert facility or the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```

/* ***** */
/* EX NR: 12192 */
/* TITLE: PERCENTAGE OF TIME IN SLOWDOWN EXCEEDS LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
IF NINCODE = 109 OR NINCODE 1109
THEN DO;
  ID =NETNAME;
  EXCCODE='12192'; SEVERITY='C'; MGMTAREA='PERFORMANCE';
  IF NINTYPE EQ 'E' THEN DO;
    EXCDDESC1 =
      'PERCENTAGE OF TIME IN SLOWDOWN EXCEEDS LIMIT' ||
      ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
    EXCDDESC2= 'HI LIM=' || TRIM(PUT(NINNRHIC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRRVAL,8.));
  END;
ELSE DO;
  EXCDDESC1 =
    'PERCENTAGE OF TIME IN SLOWDOWN EXCEEDS LIMIT' ||
    ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
  EXCDDESC2= 'HI LIM=' || TRIM(PUT(NINNRHIC,8.)) ||
    ',WAS=' || TRIM(PUT(NINNRRVAL,8.)) ||
    ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
END;
LINK HIT;

```

END;

THRESHOLD MODIFICATION: Modify thresholds in the CA NetSpy ALERTPRM member or in the NPM START MONITOR command.

12193: Percentage of Bytes Retransmitted Exceeds Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
 MANAGEMENT AREA: Performance (MGMTAREA='Performance')

PURPOSE: Identifies NPM intervals during which the percentage of total characters retransmitted out of the total characters sent exceeds installation-defined levels for a communication link or physical unit described by the element NETNAME (Resource Network Name).

RATIONALE: Both throughput and end-user response time are adversely affected by retransmissions. Typically, no links operate totally error-free over any macroscopic time period. The retransmission rate may be affected by the links's constant and transient conditions, by the line speed, and by the following NCP operands, which control such factors as maximum message size and number of messages sent before receipt of an acknowledgment: MAXDATA, MAXOUT, and PASSLIM of the PU macro and the RETRIES operand of the SDLCST macro.

Sudden significant increases in retransmissions may indicate a failing component on the link. Gradual increases in the retransmission rate may indicate that the NCP parameters for the link should be reevaluated.

DEFINITION: This exception condition is met when the number of retransmissions exceeds installation-defined thresholds for the percentage of retransmitted characters to total traffic.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12193 */
/* TITLE: PERCENTAGE OF BYTES RETRANSMITTED EXCEEDED */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
```

```
IF NINCODE = 111 THEN OR NINCODE = 1111
  THEN DO;
    ID =NETNAME;
```

```
EXCCODE='12193'; SEVERITY='I'; MGMTAREA='PERFORMANCE';
IF NINTYPE EQ 'E' THEN DO;
  EXCDESC1=
    'PERCENTAGE OF BYTES RETRANSMITTED EXCEEDS LIMIT' ||
    ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
  EXCDESC2= 'HI LIM=' || TRIM(PUT(NINNRRHIC,8.)) ||
    ',WAS=' || TRIM(PUT(NINNRRVAL,8.));
END;
ELSE DO;
  EXCDESC1=
    'PERCENTAGE OF BYTES RETRANSMITTED EXCEEDS LIMIT' ||
    ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
  EXCDESC2= 'HI LIM=' || TRIM(PUT(NINNRRHIC,8.)) ||
    ',WAS=' || TRIM(PUT(NINNRRVAL,8.)) ||
    ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
END;
LINK HIT;
END;
```

THRESHOLD MODIFICATION: Modify thresholds in the CRITERIA operand of the NPM START MONITOR command.

12194: Percentage of NCP Buffers Used Exceeds Limit

FILE: Network Incident
SAS FILE NAME: DETAIL.SNTNIN01
SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Critical (SEVERITY='C')
MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects high NCP storage usage.

RATIONALE: High percentage of NCP buffers used indicates a trend toward NCP buffer congestion, SLOWDOWN. This exception may occur with other exceptions that give an indication of the source of the congestion:

- o Processor or Messages Per Minute Overload -
Indicates a trend toward queue overloading due to high network processor CPU time.
- o Bytes Per Second or Network Component (Line) Overload -
Indicates a trend toward queue overloading due to line saturation. This overuse may be general across all lines on the processor. If the overload is localized to a few lines, the line overload exception will appear. Examine the distribution of logical units (LUs) across lines for possible load distribution improvements.
- o Percentage of Time in Slowdown Exceeds Limit -
System definitions may cause NCP slowdown conditions. Examine network parameters, such as pacing, and other environmental descriptors, such as the service order table, for possible improvements.
- o Outbound Queue Length Overload -
The free buffer percentage exception indicates a processor loading trend which may lead to outbound queue length overloads. This situation may be caused by bursts of output from host teleprocessing monitors. Such bursts may result from operating system dispatching priority or job mix imbalances. Examine host areas for hardware, SCP, or teleprocessing monitor internal bottlenecks, such as:
 - DASD device or channel contention
 - High batch activity during peak TP hours
 - CICS MAXTASK, SOS, or storage fragmentation
 - CICS journal overloads
 - IMS transaction scheduling contentions

DEFINITION: This exception is detected by either the CA NetSpy general alert facility or the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12194 */
/* TITLE: PERCENTAGE OF NCP BUFFERS USED EXCEEDS LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
```

```
IF NINCODE = 113 OR NINCODE = 1113
  THEN DO;
    ID =NETNAME;
    EXCCODE='12194'; SEVERITY='C'; MGMTAREA='PERFORMANCE';
    IF NINTYPE EQ 'E' THEN DO;
      EXCDDESC1 =
        'PERCENTAGE OF NCP BUFFERS USED EXCEEDS LIMIT' ||
        ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
      EXCDDESC2= 'HI LIM=' || TRIM(PUT(NINNRLLOC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRRVAL,8.));
    END;
  ELSE DO;
    EXCDDESC1 =
      'PERCENTAGE OF NCP BUFFERS USED EXCEEDS LIMIT' ||
      ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
    EXCDDESC2= 'HI LIM=' || TRIM(PUT(NINNRLLOC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRRVAL,8.)) ||
      ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
  END;
  LINK HIT;
END;
```

THRESHOLD MODIFICATION: Modify thresholds in the CA NetSpy ALERTPRM member or in the NPM START MONITOR command.

12195: Percentage of NCP Buffers Used Below Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Warning (SEVERITY='W')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects NCP storage underutilized

RATIONALE: If NCP buffer usage is consistently low, e.g., less than 25 percent most of the time, then an NCP may be configured for excessive storage or workloads may be disproportionate across the NCPs in the network.

DEFINITION: This exception is detected by either the CA NetSpy general alert facility or the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12195 */
/* TITLE: PERCENTAGE OF NCP BUFFERS USED BELOW LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
```

```
IF NINCODE = 112 OR NINCODE = 1112
  THEN DO;
    ID =NETNAME;
    EXCCODE='12195'; SEVERITY='W'; MGMTAREA='PERFORMANCE';
    IF NINTYPE EQ 'E' THEN DO;
      EXCDISC1 =
        'PERCENTAGE OF NCP BUFFERS USED BELOW LIMIT' ||
        ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
      EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRLV,8.));
    END;
  ELSE DO;
    EXCDISC1 =
      'PERCENTAGE OF NCP BUFFERS USED BELOW LIMIT' ||
      ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
      EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRLV,8.)) ||
        ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
    END;
```

LINK HIT;
END;

THRESHOLD MODIFICATION: Modify thresholds in the CA NetSpy
ALERTPRM member or in the NPM START MONITOR command.

12196: Transmit Bytes Per Second Below Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Warning (SEVERITY='W')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects Line, PU, LU, Phylink, and Loglink underutilization.

RATIONALE: If the resource usage is consistently low, then the resource may be overconfigured for excessive capacity anticipating a heavy workload.

DEFINITION: This exception is detected by the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12196 */
/* TITLE: TRANSMIT BYTES PER SECOND BELOW LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
```

```
IF NINCODE = 122 OR NINCODE = 1122
  THEN DO;
    ID =NETNAME;
    EXCCODE='12196'; SEVERITY='W'; MGMTAREA='PERFORMANCE';
    IF NINTYPE EQ 'E' THEN DO;
      EXCDISC1 =
        'TRANSMIT BYTES PER SECOND BELOW LIMIT ' ||
        ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
      EXCDISC2= ' LOW LIM=' || TRIM(PUT(NINNRLLOC,8.)) ||
        ', WAS=' || TRIM(PUT(NINNRRVAL,8.));
    END;
  ELSE DO;
    EXCDISC1 =
      'TRANSMIT BYTES PER SECOND BELOW LIMIT ' ||
      ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
      EXCDISC2= ' LOW LIM=' || TRIM(PUT(NINNRLLOC,8.)) ||
        ', WAS=' || TRIM(PUT(NINNRRVAL,8.)) ||
        ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
    END;
  END;
```

LINK HIT;
END;

THRESHOLD MODIFICATION: Modify thresholds in the NPM START
MONITOR command.

12197: Transmit Bytes Per Second Exceeds Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Critical (SEVERITY='C')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects Line, PU, LU, Phylink, and Loglink overutilization.

RATIONALE: If the resource usage is consistently high then the resource may be underconfigured for the current workload.

DEFINITION: This exception is detected by the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12197 */
/* TITLE: TRANSMIT BYTES PER SECOND EXCEEDS LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
```

```
IF NINCODE = 123 OR NINCODE = 1123
  THEN DO;
    ID =NETNAME;
    EXCCODE='12197'; SEVERITY='C'; MGMTAREA='PERFORMANCE';
    IF NINTYPE EQ 'E' THEN DO;
      EXCDDESC1 =
        'TRANSMIT BYTES PER SECOND EXCEEDS LIMIT ' ||
        ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
      EXCDDESC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRRVAL,8.));
    END;
  ELSE DO;
    EXCDDESC1 =
      'TRANSMIT BYTES PER SECOND EXCEEDS LIMIT ' ||
      ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
    EXCDDESC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRRVAL,8.)) ||
      ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
  END;
  LINK HIT;
```

END;

THRESHOLD MODIFICATION: Modify thresholds in the NPM
START MONITOR command.

12198: Receive Bytes Per Second Below Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Warning (SEVERITY='W')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects Line, PU, LU, Phylink, and Loglink underutilization.

RATIONALE: If the resource usage is consistently low, then the resource may be overconfigured for excessive capacity anticipating a heavy workload.

DEFINITION: This exception is detected by the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12198 */
/* TITLE: RECEIVE BYTES PER SECOND BELOW LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
```

```
IF NINCODE = 124 OR NINCODE = 1124
  THEN DO;
    ID =NETNAME;
    EXCCODE='12198'; SEVERITY='W'; MGMTAREA='PERFORMANCE';
    IF NINTYPE EQ 'E' THEN DO;
      EXCDISC1 =
        'RECEIVE BYTES PER SECOND BELOW LIMIT ' ||
        ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
      EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRLV,8.));
    END;
  ELSE DO;
    EXCDISC1 =
      'RECEIVE BYTES PER SECOND BELOW LIMIT ' ||
      ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
      EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRLV,8.)) ||
        ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
    END;
```

LINK HIT;
END;

THRESHOLD MODIFICATION: Modify thresholds in the NPM
START MONITOR command.

12199: Receive Bytes Per Second Exceeds Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Critical (SEVERITY='C')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects Line, PU, LU, Phylink, and Loglink underutilization.

RATIONALE: If the resource usage is consistently high, then the resource may be underconfigured for the current workload.

DEFINITION: This exception is detected by the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12199 */
/* TITLE: RECEIVE BYTES PER SECOND EXCEEDS LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
```

```
IF NINCODE = 125 OR NINCODE = 1125
  THEN DO;
    ID =NETNAME;
    EXCCODE='12199'; SEVERITY='C'; MGMTAREA='PERFORMANCE';
    IF NINTYPE EQ 'E' THEN DO;
      EXCDISC1 =
        'RECEIVE BYTES PER SECOND EXCEEDS LIMIT ' ||
        ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
      EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRLV,8.));
    END;
  ELSE DO;
    EXCDISC1 =
      'RECEIVE BYTES PER SECOND EXCEEDS LIMIT ' ||
      ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
      EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRLV,8.)) ||
        ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
    END;
  LINK HIT;
```

END;

THRESHOLD MODIFICATION: Modify thresholds in the NPM START
MONITOR command.

12200: Token Ring Interface % Utilization Below Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Warning (SEVERITY='W')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects Phylink underutilization.

RATIONALE: If the resource usage is consistently low, then the resource may be overconfigured for excessive capacity anticipating a heavy workload.

DEFINITION: This exception is detected by the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12200 */
/* TITLE: TOKEN RING INTERFACE % UTILIZATION BELOW LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
```

```
IF NINCODE = 126 OR NINCODE = 1126
  THEN DO;
    ID =NETNAME;
    EXCCODE='12200'; SEVERITY='W'; MGMTAREA='PERFORMANCE';
    IF NINTYPE EQ 'E' THEN DO;
      EXCDISC1 =
        'TOKEN RING INTERFACE % UTILIZATION BELOW LIMIT' ||
        ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
      EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRLV,8.));
    END;
  ELSE DO;
    EXCDISC1 =
      'TOKEN RING INTERFACE % UTILIZATION BELOW LIMIT' ||
      ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
    EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRLV,8.)) ||
      ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
  END;
  LINK HIT;
```

END;

THRESHOLD MODIFICATION: Modify thresholds in the NPM START
MONITOR command.

12201: Token Ring Interface % Utilization Exceeds Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Critical (SEVERITY='C')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects Phylink overutilization.

RATIONALE: If the resource usage is consistently high, then the resource may be underconfigured for the heavy workload being experienced.

DEFINITION: This exception is detected by the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12201 */
/* TITLE: TOKEN RING INTERFACE % UTILIZATION EXCEEDS LMT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
```

```
IF NINCODE = 127 OR NINCODE = 1127
  THEN DO;
    ID =NETNAME;
    EXCCODE='12201'; SEVERITY='C'; MGMTAREA='PERFORMANCE';
    IF NINTYPE EQ 'E' THEN DO;
      EXCDDESC1 =
        'TOKEN RING INTERFACE % UTILIZATION EXCEEDS LIMIT' ||
        ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
      EXCDDESC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRRVAL,8.)) ||
      END;
    ELSE DO;
      EXCDDESC1 =
        'TOKEN RING INTERFACE % UTILIZATION EXCEEDS LIMIT' ||
        ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
      EXCDDESC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRRVAL,8.)) ||
        ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
      END;
    LINK HIT;
```

END;

THRESHOLD MODIFICATION: Modify thresholds in the NPM
START MONITOR command.

12202: Congestion Count Below Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Warning (SEVERITY='W')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects the number of frames that could not be copied to the token-ring adapter due to adapter congestion.

RATIONALE: If the resource usage is consistently low, then the resource may be overconfigured for excessive capacity anticipating a heavy workload.

DEFINITION: This exception is detected by the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12202 */
/* TITLE: CONGESTION COUNT BELOW LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
```

```
IF NINCODE = 128 OR NINCODE = 1128
  THEN DO;
    ID =NETNAME;
    EXCCODE='12202'; SEVERITY='W'; MGMTAREA='PERFORMANCE';
    IF NINTYPE EQ 'E' THEN DO;
      EXCDISC1 =
        'CONGESTION COUNT BELOW LIMIT' ||
        ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
      EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRLVAL,8.));
    END;
  ELSE DO;
    EXCDISC1 =
      'CONGESTION COUNT BELOW LIMIT' ||
      ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
    EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRLVAL,8.)) ||
      ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
  END;
```

LINK HIT;
END;

THRESHOLD MODIFICATION: Modify thresholds in the NPM START
MONITOR command.

12203: Congestion Count Exceeds Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Critical (SEVERITY='C')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects the number of frames that could not be copied to the token-ring adapter due to adapter congestion.

RATIONALE: If the resource usage is consistently high then the resource may be underconfigured for the heavy workload being experienced.

DEFINITION: This exception is detected by the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12203 */
/* TITLE: CONGESTION COUNT EXCEEDS LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
```

```
IF NINCODE = 129 OR NINCODE = 1129
  THEN DO;
    ID =NETNAME;
    EXCCODE='12203'; SEVERITY='C'; MGMTAREA='PERFORMANCE';
    IF NINTYPE EQ 'E' THEN DO;
      EXCDISC1 =
        'CONGESTION COUNT EXCEEDS LIMIT' ||
        ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
      EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRLVAL,8.));
    END;
  ELSE DO;
    EXCDISC1 =
      'CONGESTION COUNT EXCEEDS LIMIT' ||
      ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
    EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRLVAL,8.)) ||
      ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
  END;
```

LINK HIT;
END;

THRESHOLD MODIFICATION: Modify thresholds in the NPM
START MONITOR command.

12204: Percent Retransmitted Bytes Below Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Warning (SEVERITY='W')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects the percent of total bytes sent that were retransmitted for the Line, PU, or Phylink.

RATIONALE: If the percent of retransmitted bytes is below the limit, it could signal the fact that current maintenance has had a positive effect on the resource.

DEFINITION: This exception is detected by the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12204 */
/* TITLE: PERCENT RETRANSMITTED BYTES BELOW LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
```

```
IF NINCODE = 130 OR NINCODE = 1130
  THEN DO;
    ID =NETNAME;
    EXCCODE='12204'; SEVERITY='W'; MGMTAREA='PERFORMANCE';
    IF NINTYPE EQ 'E' THEN DO;
      EXCDISC1 =
        'PERCENT RETRANSMITTED BYTES BELOW LIMIT' ||
        ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
      EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRLVAL,8.));
    END;
  ELSE DO;
    EXCDISC1 =
      'PERCENT RETRANSMITTED BYTES BELOW LIMIT' ||
      ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
      EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRLVAL,8.)) ||
        ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
  END;
```

LINK HIT;
END;

THRESHOLD MODIFICATION: Modify thresholds in the NPM
START MONITOR command.

12205: Percent Retransmitted Bytes Exceeds Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Critical (SEVERITY='C')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects the percent of total bytes sent that were retransmitted for the Line, PU, or Phylink.

RATIONALE: If the percent of retransmitted bytes exceeds the limit it could be the source of poor response times being reported.

DEFINITION: This exception is detected by the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12205 */
/* TITLE: PERCENT RETRANSMITTED BYTES EXCEEDS LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
```

```
IF NINCODE = 131 OR NINCODE = 1131
  THEN DO;
    ID =NETNAME;
    EXCCODE='12205'; SEVERITY='C'; MGMTAREA='PERFORMANCE';
    IF NINTYPE EQ 'E' THEN DO;
      EXCDISC1 =
        'PERCENT RETRANSMITTED BYTES EXCEEDS LIMIT' ||
        ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
      EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRLVAL,8.));
    END;
  ELSE DO;
    EXCDISC1 =
      'PERCENT RETRANSMITTED BYTES EXCEEDS LIMIT' ||
      ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
      EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRLVAL,8.)) ||
        ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
  END;
```

LINK HIT;
END;

THRESHOLD MODIFICATION: Modify thresholds in the NPM
START MONITOR command.

12206: Transmit PDU Per Minute Below Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Warning (SEVERITY='W')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects the number of protocol data units that are transmitted per minute. For SDLC protocols, PDU represents a path information unit. For token-ring protocols, PDU represents an I-frame.

RATIONALE: Under normal conditions a low PSU transmit rate would not be an exception. There may be special circumstances where this could be considered an exception, e.g., if users on the token-ring are reporting poor response times and the PDU rate is low.

DEFINITION: This exception is detected by the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12206 */
/* TITLE: TRANSMIT PDU PER MINUTE BELOW LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
```

```
IF NINCODE = 132 OR NINCODE = 1132
  THEN DO;
    ID =NETNAME;
    EXCCODE='12206'; SEVERITY='W'; MGMTAREA='PERFORMANCE';
    IF NINTYPE EQ 'E' THEN DO;
      EXCDISC1 =
        'TRANSMIT PDU PER MINUTE BELOW LIMIT' ||
        ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
      EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRLVAL,8.));
    END;
  ELSE DO;
    EXCDISC1 =
      'TRANSMIT PDU PER MINUTE BELOW LIMIT' ||
      ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
```

```
EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLC,8.)) ||  
          ',WAS=' || TRIM(PUT(NINNRLV,8.)) ||  
          ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));  
END;  
LINK HIT;  
END;
```

THRESHOLD MODIFICATION: Modify thresholds in the NPM START
MONITOR command.

12207: Transmit PDU Per Minute Exceeds Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Critical (SEVERITY='C')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects the number of protocol data units that are transmitted per minute. For SDLC protocols, PDU represents a path information unit. For token-ring protocols, PDU represents an I-frame.

RATIONALE: This could indicate the beginning of a possible response time problem. When the transmit rate exceeds the threshold, it could cause response times to increase.

DEFINITION: This exception is detected by the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12207 */
/* TITLE: TRANSMIT PDU PER MINUTE EXCEEDS LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
```

```
IF NINCODE = 133 OR NINCODE = 1133
  THEN DO;
    ID =NETNAME;
    EXCCODE='12207'; SEVERITY='C'; MGMTAREA='PERFORMANCE';
    IF NINTYPE EQ 'E' THEN DO;
      EXCDDESC1 =
        'TRANSMIT PDU PER MINUTE EXCEEDS LIMIT' ||
        ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
      EXCDDESC2= 'LOW LIM=' || TRIM(PUT(NINNRLLOC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRRVAL,8.));
    END;
  ELSE DO;
    EXCDDESC1 =
      'TRANSMIT PDU PER MINUTE EXCEEDS LIMIT' ||
      ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
    EXCDDESC2= 'LOW LIM=' || TRIM(PUT(NINNRLLOC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRRVAL,8.)) ||
```

```
        ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));  
END;  
LINK HIT;  
END;
```

THRESHOLD MODIFICATION: Modify thresholds in the NPM START
MONITOR command.

12208: Receive PDU Per Minute Below Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Warning (SEVERITY='W')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects the number of protocol data units that are received per minute. For SDLC protocols, PDU represents a path information unit. For token-ring protocols, PDU represents an I-frame.

RATIONALE: Under normal conditions a low PSU receive rate would not be an exception. There may be special circumstances where this could be considered an exception.

DEFINITION: This exception is detected by the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12208 */
/* TITLE: RECEIVE PDU PER MINUTE BELOW LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
```

```
IF NINCODE = 134 OR NINCODE = 1134
  THEN DO;
    ID =NETNAME;
    EXCCODE='12208'; SEVERITY='W'; MGMTAREA='PERFORMANCE';
    IF NINTYPE EQ 'E' THEN DO;
      EXCDDESC1 =
        'RECEIVE PDU PER MINUTE BELOW LIMIT' ||
        ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
      EXCDDESC2= 'LOW LIM=' || TRIM(PUT(NINNRLLOC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRRVAL,8.));
    END;
  ELSE DO;
    EXCDDESC1 =
      'RECEIVE PDU PER MINUTE BELOW LIMIT' ||
      ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
    EXCDDESC2= 'LOW LIM=' || TRIM(PUT(NINNRLLOC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRRVAL,8.)) ||
```

```
        ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));  
END;  
LINK HIT;  
END;
```

THRESHOLD MODIFICATION: Modify thresholds in the NPM START
MONITOR command.

12209: Receive PDU Per Minute Exceeds Limit

FILE: Network Incident
 SAS FILE NAME: DETAIL.SNTNIN01
 SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Critical (SEVERITY='C')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Detects the number of protocol data units that are received per minute. For SDLC protocols, PDU represents a path information unit. For token-ring protocols, PDU represents an I-frame.

RATIONALE: This can indicate unusually high activity and signal possible errors or poor response time problems.

DEFINITION: This exception is detected by the NPM exception monitor.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12209 */
/* TITLE: RECEIVE PDU PER MINUTE ABOVE LIMIT */
/* FILE: DETAIL.SNTNIN01 */
/* ***** */
```

```
IF NINCODE = 135 OR NINCODE = 1135
  THEN DO;
    ID =NETNAME;
    EXCCODE='12209'; SEVERITY='C'; MGMTAREA='PERFORMANCE';
    IF NINTYPE EQ 'E' THEN DO;
      EXCDISC1 =
        'RECEIVE PDU PER MINUTE ABOVE LIMIT' ||
        ',NCP=' || NCPNAME || ',XRES=' || NINRESOL;
      EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLLOC,8.)) ||
        ',WAS=' || TRIM(PUT(NINNRRVAL,8.));
    END;
  ELSE DO;
    EXCDISC1 =
      'RECEIVE PDU PER MINUTE ABOVE LIMIT' ||
      ',NCP=' || NCPNAME || ',REASON=' || NINEXCRC;
    EXCDISC2= 'LOW LIM=' || TRIM(PUT(NINNRLLOC,8.)) ||
      ',WAS=' || TRIM(PUT(NINNRRVAL,8.)) ||
      ',INTV=' TRIM(LEFT(PUT(NINNREXI,3.)));
```

```
END;  
LINK HIT;  
END;
```

THRESHOLD MODIFICATION: Modify thresholds in the NPM START
MONITOR command.

12301: Response Objective Missed For Performance Class

FILE: NLDM Service
 SAS FILE NAME: DETAIL.SNTNSV01;
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
 MANAGEMENT AREA: Performance (MGMTAREA='PERFORMANCE')

PURPOSE: Identify those (NLDM) Performance Classes for which response time objectives were missed.

RATIONALE: Control units (3274s) with the Response Time Monitor feature installed measure end-user response time for terminal sessions. This unique feature also allows you to specify response time objectives as the percentage of all transactions being less than a predetermined value (in seconds). For example, an installation determines that the terminals attached to control unit XYZ would provide adequate service if 90 percent of all transactions have end-user response times under three seconds. These objectives are defined to NLDM and the control unit. If, during a predefined interval (such as 30 minutes), that objective is not met, the control unit and NLDM record the objective as missed.

Response objectives are related to NLDM performance classes. A performance class constitutes any grouping the installation chooses. For example, all users on the same link may belong to a performance class; or all TSO users may belong to a performance class. The installation defines the performance class service objectives, then maps the terminal sessions to the appropriate performance classes using the NLDM MAPSESS command.

DEFINITION: This exception is detected when the NLDM/RTM response objective met flag has a value of 'N'.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12301 */
/* TITLE: TOTAL RESPONSE OBJ MISSED */
/* FILE: DETAIL.SNTNSV01 */
/* ***** */
```

```
IF NSVNRROM NE ONE THEN DO;
  ID =NSVPCLSS;
  EXCCODE='12301'; SEVERITY='I'; MGMTAREA='SERVICE';
  EXCDDESC1=
    'RESPONSE OBJECTIVE MISSED FOR PERFORMANCE CLASS ' ;
  EXCDDESC2=PLU || '/' || SLU ||
    ', OBJ %= ' || TRIM(LEFT(PUT(NSVPCOBJ,PERCENT.))) ||
    ', RESP OBJ TIME= ' ||
    TRIM(LEFT(PUT(NSVR0BTM,TIME9.1)));
  LINK HIT;
END;
```

THRESHOLD MODIFICATION: Perform threshold modification
in NLDM and/or 3274 customization.

12541: NPDA Event

NPDA Event
 DETAIL.SNTNEF01;
 prefix.MICS.USER.SOURCE(DYSNTEXC)

Critical (SEVERITY='C')
 Service (MGMTAREA='SERVICE')

PURPOSE: Identifies those network components potentially having problems.

RATIONALE: Network components can have problems for many reasons. NPDA monitors all components for hard and soft failures and records events that may affect network components. These events may range from temporary control unit errors to complete link (line) failures.

DEFINITION: Events are recorded in the NPDA Report record. All records which document NPDA events are recorded in this exception.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12541 */
/* TITLE: NPDA EVENT */
/* FILE: DETAIL.SNTNEF01 */
/* **NOTE : EACH RECORD ON THIS FILE REPRESENTS AN EVENT */
/* ***** */
```

```
ID =NEFFRNAM;
EXCCODE='12541'; SEVERITY='C'; MGMTAREA='SERVICE';
EXCDISC1='NPDA EVENT FOR ' || NEFFRTYP ;
EXCDISC2='PROB CAUSE:' || NEFFRDS;
LINK HIT;
```

THRESHOLD MODIFICATION: Statistics (temporary errors) are recorded as events when their error-to-traffic ratios exceed installation-defined thresholds. These thresholds are specified by resource types (LINE, CTRL, LCTL, or LDEV) and resource name either during NPDA installation (on the 'R' statement in the BNJMBDST member in the NCCF Definition Data Set) or by using the NPDA command SRATIO.

12542: NPDA Event Alert

FILE: NPDA Event
SAS FILE NAME: DETAIL.SNTNEF01;
SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Critical (SEVERITY='C')
MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies those network components with problems serious enough to be considered for immediate ALERT notification.

RATIONALE: NPDA allows you to specify certain events as critical in nature by flagging the event as an alert. As a result, any NPDA operators monitoring alerts are immediately notified and an NPDA reports record is created to document this potentially severe problem.

DEFINITION: This exception is detected if the NPDA alert flag is set.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */  
/* EX NR: 12542 */  
/* TITLE: NPDA EVENT ALERT */  
/* FILE: DETAIL.SNTNEF01 */  
/* ***** */
```

```
IF NEFNRLT=ONE THEN DO;  
  ID =NEFFRNAM;  
  EXCCODE='12542'; SEVERITY='C'; MGMTAREA='SERVICE';  
  EXCDISC1='NPDA EVENT ALERT FOR ' || NEFFRTYP ;  
  EXCDISC2='PROB CAUSE:' || NEFFERRDS;  
  LINK HIT;  
END;
```

THRESHOLD MODIFICATION: Use the SRFILTER AREC command to establish the criteria by which specific events are flagged as alerts.

12601: NPDA Statistical Alert

FILE: NPDA Statistical
 SAS FILE NAME: DETAIL.SNTNSF01;
 SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Critical (SEVERITY='C')
 MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies those network components potentially having problems.

RATIONALE: NPDA allows you to monitor temporary errors for network components and record those errors as statistics. When the ratio of error-to-traffic exceeds a user-defined threshold, the statistic becomes an event. An event becomes an alert due to installation-defined criteria. These occurrences of statistical alerts are recorded by this exception.

DEFINITION: This exception is detected if the NPDA alert flag is set in the NPDA Reports record, which indicates the occurrence of a recurring temporary error condition.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */
/* EX NR: 12601 */
/* TITLE: NPDA ALERT */
/* FILE: DETAIL.SNTNSF01 */
/* ***** */
```

```
IF NSFNRLT=ONE THEN DO;
  ID =NSFFRNAM;
  EXCCODE='12601'; SEVERITY='C'; MGMTAREA='SERVICE';
  EXCDISC1='NPDA STATISTICAL ALERT FOR ' || NSFFRTYP ;
  EXCDISC2='TOTAL TRAFFIC:' || TRIM(PUT(NSFTTRFC,8.)) ||
  ',TOTAL TEMPORARY ERRORS:' || TRIM(PUT(NSFTTERR,8.));
  LINK HIT;
END;
```

THRESHOLD MODIFICATION: Perform threshold modification in NPDA using the SRFILTER AREC command.

12661: Host Response Outside Bounds-Count Exceeded for SLU

FILE: NPM User Activity
SAS FILE NAME: DETAIL.SNTPSU01;
SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies those NPM intervals during which end-user response time may have been poor due to host turnaround.

RATIONALE: End-user response time is divided into two categories by NPM:

- o Host response time - the amount of time required for the host hardware and software to service a request (or transaction). This includes VTAM time and host application time.
- o Network response time - the amount of time required for the network to service a request. This typically includes link transmission time, time in the control unit, and any time a request is queued by the communications controller.

NPM allows you to specify high and low bounds for acceptable host response time. If actual response time falls outside those bounds, NPM increments the host response exceeded counter by one.

DEFINITION: This exception is detected if the count of occurrences of host response time outside installation-defined bounds is exceeded. Note that there are thresholds you can set in NPM and also a threshold count set in this exception process that result in the exception being generated.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */  
/* EX NR: 12661 */  
/* TITLE: HOST RESPONSE EXCEEDED COUNT THRESHOLD EXCEEDED */  
/* (NPM MAINTAINS RESPONSE EXCEEDED COUNTERS FOR */  
/* (ALL RESPONSES THAT FALL OUTSIDE NPM SPECIFIED */  
/* (PARAMETERS). */
```

```

/* FILE:  DETAIL.SNTPSU01                                     */
/* ***** */

T_NRHRE=5; /* CHG THIS STATEMENT TO ADJUST THE THRESHOLD */
IF PSUNRHRE GT T_NRHRE THEN DO;
  ID =SLU;
  EXCCODE='12661'; SEVERITY='I'; MGMTAREA='SERVICE';
  EXCDESC1=
    'HOST RESP OUTSIDE BOUNDS-COUNT EXCEEDED FOR SLU ' ;
  EXCDESC2='PLU= ' || PLU ||
    ' .  LOW T.H.= ' || TRIM(LEFT(PUT(NPMLHST,8.))) ||
    ', HI T.H.= ' || TRIM(LEFT(PUT(NPMHIHST,8.))) ||
    ', CNT= ' || TRIM(LEFT(PUT(PSUNRHRE,8.))) ||
    ', CNT LIMIT= ' || TRIM(LEFT(PUT(T_NRHRE,8.))) ;
  LINK HIT;
END;

```

THRESHOLD MODIFICATION: Modify the value of T_NRHRE to represent the installation-defined host response exceeded count threshold. To establish the NPM threshold boundaries (low and high) for host response time, use the HOST operand of the NPM SESSCOLL command.

12662: Net Response Outside Bounds-Count Exceeded for SLU

FILE: NPM User Activity
SAS FILE NAME: DETAIL.SNTPSU01;
SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies those NPM intervals during which end-user response time may have been poor due to network service.

RATIONALE: End-user response time is divided into two categories by NPM:

- o Host response time - the amount of time required for the host hardware and software to service a request (or transaction). This includes VTAM time and host application time.
- o Network response time - the amount of time required for the network to service a request. This typically includes link transmission time, time in the control unit, and any time the request was queued by the communications controller.

NPM allows you to specify high and low bounds for acceptable network response time. If actual response time falls outside those bounds, NPM increments the network response exceeded counter by one.

DEFINITION: This exception is detected if the count of occurrences of network response time outside installation-defined bounds is exceeded. Note that there are thresholds you can set in NPM and also a threshold count set in this exception process that result in the exception being generated.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */  
/* EX NR: 12662 */  
/* TITLE: NET RESPONSE EXCEEDED COUNT THRESHOLD EXCEEDED */  
/* (NPM MAINTAINS RESPONSE EXCEEDED COUNTERS FOR */  
/* (ALL RESPONSES THAT FALL OUTSIDE NPM SPECIFIED */  
/* (PARAMETERS). */
```

```

/* FILE:  DETAIL.SNTPSU01                                     */
/* ***** */

T_NNRNRE=5; /* CHG THIS STATEMENT TO ADJUST THE THRESHOLD */
IF PSUNRNRE GT T_NNRNRE THEN DO;
  ID =SLU;
  EXCCODE='12662'; SEVERITY='I'; MGMTAREA='SERVICE';
  EXCDDESC1=
    'NET RESP OUTSIDE BOUNDS-COUNT EXCEEDED FOR SLU ' ;
  EXCDDESC2='PLU= ' || PLU ||
    ' .  LOW T.H.= ' || TRIM(LEFT(PUT(NPMLONET,8.))) ||
    ' , HI T.H.= ' || TRIM(LEFT(PUT(NPMHINET,8.))) ||
    ' , CNT= ' || TRIM(LEFT(PUT(PSUNRNRE,8.))) ||
    ' , CNT LIMIT= ' || TRIM(LEFT(PUT(T_NNRNRE,8.))) ;
  LINK HIT;
END;

```

THRESHOLD MODIFICATION: Modify the value of T_NNRNRE to represent the installation-defined network response exceeded count threshold. To establish the NPM threshold boundaries (low and high) for network response time, use the NET operand of the NPM SESSCOLL command.

12663: Total Response Outside Bounds-Count Exceeded for SLU

FILE: NPM User Activity
SAS FILE NAME: DETAIL.SNTPSU01;
SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies those NPM intervals during which end-user total response time was poor.

RATIONALE: End-user response time is divided into two categories by NPM:

- o Host response time - the amount of time required for the host hardware and software to service a request (or transaction). This includes VTAM time and host application time.
- o Network response time - the amount of time required for the network to service a request. This typically includes link transmission time, time in the control unit, and any time during which the request is queued by the communications controller.

Whenever NPM is unable to record network response time, it applies the average network response time for transactions for which it was able to record network response. Total response time is the combination of host response time, network response time, and calculated network response time.

NPM allows you to specify high and low bounds for acceptable total response time (also known as operator time in NPM). If actual response time falls outside those bounds, NPM increments the total (operator) response exceeded counter by one.

DEFINITION: This exception is detected if the count of occurrences of total response time outside installation-defined bounds is exceeded. Note that there are thresholds you can set in NPM and also a threshold count set in this exception process that result in the exception being generated.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:


```

/* ***** */
/* EX NR: 12663 */
/* TITLE: TOTAL RESPONSE EXCEEDED COUNT THRESHOLD */
/* EXCEEDED. */
/* (NPM MAINTAINS RESPONSE EXCEEDED COUNTERS FOR */
/* (ALL RESPONSES THAT FALL OUTSIDE NPM SPECIFIED */
/* (PARAMETERS). */
/* FILE: DETAIL.SNTPSU01 */
/* ***** */

```

```

T_NRTRE=1; /* CHG THIS STATEMENT TO ADJUST THE THRESHOLD */
IF PSUNRTRE GT T_NRNRE THEN DO;
  ID =SLU;
  EXCCODE='12663'; SEVERITY='I'; MGMTAREA='SERVICE';
  EXCDDESC1=
    'TOTAL RESP OUTSIDE BOUNDS-COUNT EXCEEDED FOR SLU ' ;
  EXCDDESC2='PLU= ' || PLU ||
    ' . LOW T.H.= ' || TRIM(LEFT(PUT(NPMLTOT,8.))) ||
    ', HI T.H.= ' || TRIM(LEFT(PUT(NPMHITOT,8.))) ||
    ', CNT= ' || TRIM(LEFT(PUT(PSUNRTRE,8.))) ||
    ', CNT LIMIT= ' || TRIM(LEFT(PUT(T_NRTRE,8.))) ;
  LINK HIT;
END;

```

THRESHOLD MODIFICATION: Modify the value of T_NRHTE to represent the installation-defined total response exceeded count threshold. To establish the NPM threshold boundaries (low and high) for total response time, use the OPER operand of the NPM SESSCOLL command.

12780: Host Response Outside Bounds-Count Exceeded for Link

FILE: NPM Link Activity
SAS FILE NAME: DETAIL.SNTNPL01;
SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies those NPM intervals during which end-user response time may have been poor due to host turnaround.

RATIONALE: End-user response time is divided into two categories by NPM:

- o Host response time - the amount of time required for the host hardware and software to service a request (or transaction). This includes VTAM time and host application time.
- o Network response time - the amount of time required for the network to service a request. This typically includes link transmission time, time in the control unit, and any time during which the request is queued by the communications controller.

NPM allows you to specify high and low bounds for acceptable host response time. If actual response time falls outside those bounds, NPM increments the host response exceeded counter by one.

DEFINITION: This exception is detected if the count of occurrences of host response time outside installation-defined bounds is exceeded. Note that there are thresholds you can set in NPM and also a threshold count set in this exception process that result in the exception being generated.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */  
/* EX NR: 12780 */  
/* TITLE: HOST RESPONSE EXCEEDED COUNT THRESHOLD EXCEEDED */  
/* FOR A LINK. */  
/* (NPM MAINTAINS RESPONSE EXCEEDED COUNTERS FOR */
```

```

/*      (ALL RESPONSES THAT FALL OUTSIDE NPM SPECIFIED  */
/*      (PARAMETERS).                                     */
/* FILE:  DAYS.SNTNPL01                                   */
/* ***** */

T_NRHRE=32; /* CHG THIS STATEMENT TO ADJUST THE THRESHOLD */
IF NPLNRHRE GT T_NRHRE THEN DO;
  ID =SLULINK;
  EXCCODE='12780'; SEVERITY='I'; MGMTAREA='SERVICE';
  EXCDDESC1=
    'HOST RESP OUTSIDE BOUNDS-COUNT EXCEEDED FOR LINK' ;
  EXCDDESC2=
    '.  LOW T.H.= ' || TRIM(LEFT(PUT(NPMLOHST,8.))) ||
    ', HI T.H.= ' || TRIM(LEFT(PUT(NPMHIHST,8.))) ||
    ', CNT= ' || TRIM(LEFT(PUT(NPLNRHRE,8.))) ||
    ', CNT LIMIT= ' || TRIM(LEFT(PUT(T_NRHRE,8.))) ;
  LINK HIT;
END;

```

THRESHOLD MODIFICATION: Modify the value of T_NRHRE to represent the installation-defined host response exceeded count threshold. To establish the NPM threshold boundaries (low and high) for host response time, use the HOST operand of the NPM SESSCOLL command.

12781: Network Response Outside Bounds-Count Exceeded for Link

FILE: NPM Link Activity
SAS FILE NAME: DETAIL.SNTNPL01;
SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies those NPM intervals during which end-user response time may have been poor due to network service.

RATIONALE: End-user response time is divided into two categories by NPM:

- o Host response time - the amount of time required for the host hardware and software to service a request (or transaction). This includes VTAM time and host application time.
- o Network response time - the amount of time required for the network to service a request. This typically includes link transmission time, time in the control unit, and any time during which the request is queued by the communications controller.

NPM allows you to specify high and low bounds for acceptable network response time. If actual response time falls outside those bounds, NPM increments the network response exceeded counter by one.

DEFINITION: This exception is detected if the count of occurrences of network response time outside installation-defined bounds is exceeded. Note that there are thresholds you can set in NPM and also a threshold count set in this exception process that result in the exception being generated.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */  
/* EX NR: 12781 */  
/* TITLE: NET RESPONSE EXCEEDED COUNT THRESHOLD EXCEEDED */  
/* FOR A LINK. */  
/* (NPM MAINTAINS RESPONSE EXCEEDED COUNTERS FOR */
```

```

/*      (ALL RESPONSES THAT FALL OUTSIDE NPM SPECIFIED  */
/*      (PARAMETERS).                                     */
/* FILE:  DAYS.SNTNPL01                                   */
/* ***** */

T_NRNRE=4; /* CHG THIS STATEMENT TO ADJUST THE THRESHOLD */
IF NPLNRNRE GT T_NRNRE THEN DO;
  ID =SLULINK;
  EXCCODE='12781'; SEVERITY='I'; MGMTAREA='SERVICE';
  EXCDDESC1=
    'NET RESP OUTSIDE BOUNDS-COUNT EXCEEDED FOR LINK' ;
  EXCDDESC2=
    ' .  LOW T.H.= ' || TRIM(LEFT(PUT(NPMLONET,8.))) ||
    ', HI T.H.= ' || TRIM(LEFT(PUT(NPMHINET,8.))) ||
    ', CNT= ' || TRIM(LEFT(PUT(NPLNRNRE,8.))) ||
    ', CNT LIMIT= ' || TRIM(LEFT(PUT(T_NRNRE,8.))) ;
  LINK HIT;
END;

```

THRESHOLD MODIFICATION: Modify the value of T_NRNRE to represent the installation-defined network response exceeded count threshold. To establish the NPM threshold boundaries (low and high) for network response time, use the NET operand of the NPM SESSCOLL command.

12782: Total Response Outside Bounds-Count Exceeded for Link

FILE: NPM Link Activity
SAS FILE NAME: DETAIL.SNTNPL01;
SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies those NPM intervals during which end-user total response time was poor.

RATIONALE: End-user response time is divided into two categories by NPM:

- o Host response time - the amount of time required for the host hardware and software to service a request (or transaction). This includes VTAM time and host application time.
- o Network response time - the amount of time required for the network to service a request. This typically includes link transmission time, time in the control unit, and any time during which the request is queued by the communications controller.

NPM allows you to specify high and low bounds for acceptable total response time. If actual response time falls outside those bounds, NPM increments the total response exceeded counter by one.

DEFINITION: This exception is detected if the count of occurrences of total response time outside installation-defined bounds is exceeded. Note that there are thresholds you can set in NPM and also a threshold count set in this exception process that result in the exception being generated.

EXCEPTION STATEMENTS: The SAS statements identifying the exception situation and describing the condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** */  
/* EX NR: 12782 */  
/* TITLE: TOTAL RESPONSE EXCEEDED COUNT THRESHOLD */  
/* EXCEEDED FOR A LINK */  
/* (NPM MAINTAINS RESPONSE EXCEEDED COUNTERS FOR */  
/* (ALL RESPONSES THAT FALL OUTSIDE NPM SPECIFIED */
```

```

/*          (PARAMETERS).          */
/* FILE:  DAYS.SNTNPL01          */
/* *****          */

T_NRTRE=6; /* CHG THIS STATEMENT TO ADJUST THE THRESHOLD */
IF NPLNRTRE GT T_NRNRE THEN DO;
  ID =SLULINK;
  EXCCODE='12782'; SEVERITY='I'; MGMTAREA='SERVICE';
  EXCDESC1=
    'TOTAL RESP OUTSIDE BOUNDS-COUNT EXCEEDED FOR LINK' ;
  EXCDESC2=
    ' . LOW T.H.= ' || TRIM(LEFT(PUT(NPMLTOT,8.))) ||
    ', HI T.H.= ' || TRIM(LEFT(PUT(NPMHITOT,8.))) ||
    ', CNT= ' || TRIM(LEFT(PUT(NPLNRTRE,8.))) ||
    ', CNT LIMIT= ' || TRIM(LEFT(PUT(T_NRTRE,8.))) ;
  LINK HIT;
END;

```

THRESHOLD MODIFICATION: Modify the value of T_NRHTE to represent the installation-defined total response exceeded count threshold. To establish the NPM threshold boundaries (low and high) for total response time, use the OPER operand of the NPM SESSCOLL command.

12801: Response Objective Missed for APPL/PCLASS

FILE: NLDM System (PLU) Activity
SAS FILE NAME: DAYS.NVSLSY01;
SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies performance classes that have exceeded installation-defined thresholds for response time.

RATIONALE: High response times for a performance class indicate that certain users (who are identified by performance class value) for the selected application are not receiving satisfactory service.

DEFINITION: The exception condition is met when response time exceeds installation-defined thresholds.

EXCEPTION STATEMENTS: The SAS statements that identify this exception condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* *****  
/* EX NR: 12801  
/* TITLE: TOTAL RESPONSE OBJ MISSED  
/* FILE: DAYS.NVSLSY01  
/* *****
```

```
T_OBJPCT=70; /* USER DEFINED PERCENT OBJECTIVE */  
IF LSYP COBM LT T_OBJPCT THEN DO;  
  ID =PLU;  
  EXCCODE='12801'; SEVERITY='I'; MGMTAREA='SERVICE';  
  EXCDESC1=  
    'RESPONSE OBJECTIVE MISSED FOR APPL/PCLASS.';  
  EXCDESC2='APPL/PCLASS: ' || PLU || '/' || PERFCLSS ||  
    ', OBJ %=' || TRIM(LEFT(PUT(T_OBJPCT,PERCENT.))) ||  
    ', ACTUAL %=' ||  
    TRIM(LEFT(PUT(LSYP COBM,PERCENT.)));  
  LINK HIT;  
END;
```

THRESHOLD MODIFICATION: Modify the value of T_OBJPCT to represent the user-defined performance class threshold.

12802: Response Objective Missed for LINK/PCLASS

FILE: NLDL Link Activity
 SAS FILE NAME: DAYS.NVSNLL01;
 SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
 MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies performance classes that have exceeded installation-defined thresholds for link response time.

RATIONALE: High response times for a performance class indicate that certain users (who are identified by performance class value) for the selected link are not receiving satisfactory service.

DEFINITION: The exception condition is met when response time exceeds installation-defined thresholds.

EXCEPTION STATEMENTS: The SAS statements that identify this exception condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* ***** * /
/* EX NR: 12802 * /
/* TITLE: TOTAL RESPONSE OBJ MISSED * /
/* FILE: DAYS.NVSNLL01 * /
/* ***** * /
```

```
T_OBJPCT=70; /* USER DEFINED PERCENT OBJECTIVE */
IF NLLPCOBM LT T_OBJPCT THEN DO;
  ID =PLU;
  EXCCODE='12802'; SEVERITY='I'; MGMTAREA='SERVICE';
  EXCDESC1=
    'RESPONSE OBJECTIVE MISSED FOR LINK/PCLASS.';
  EXCDESC2='LINK/PCLASS: ' || SLULINK || '/' || PERFLSS ||
    ', OBJ %= ' || TRIM(LEFT(PUT(T_OBJPCT,PERCENT.))) ||
    ', ACTUAL %= ' ||
    TRIM(LEFT(PUT(NLLPCOBM,PERCENT.)));
  LINK HIT;
END;
```

THRESHOLD MODIFICATION: Modify the value of T_OBJPCT to represent the user-defined performance class threshold for the links.

12852: Invalid Session Parameters Threshold Exceeded

FILE: NLDM VTAM BIND Failure
SAS FILE NAME: DAYS.NVSVBF01
SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies the hours that have exceeded installation-defined thresholds for the number of UNBIND failures due to an "Invalid Session Parameters" condition.

RATIONALE: An abnormal UNBIND is a disruptive termination of a terminal user's session with the host application. A large number of UNBINDs indicates problems with either the application or the network components used to access the application. An abnormal UNBIND can occur any time except normal session end, or when one application is passing a terminal session to another application.

DEFINITION: The exception condition is met when the number of failures exceeds installation-defined thresholds.

EXCEPTION STATEMENTS: The SAS statements that identify this exception condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* *****  
/* EX NR: 12852  
/* TITLE: INVALID SESSION PARAMETERS THRESHOLD EXCEEDED */  
/* FILE: DAYS.NVSVBF01  
/* *****  
  
IF VBFRCODE='06' AND VBFNRBF GT UN_HEX06 THEN DO;  
  ID =SLU;  
  EXCCODE='12852'; SEVERITY='I'; MGMTAREA='SERVICE';  
  EXCDISC1=  
    'INVALID SESSION PARAMETERS  
THRESHOLD EXCEEDED.';  
  EXCDISC2='PLU/SLU= ' || PLU || '/' || SLU ||  
    ', THRESHOLD= ' || PUT(UN_HEX06,COMMA6.) ||  
    ', NUMBER FOUND= ' || PUT(VBFNRBF,COMMA6.) ;  
  LINK HIT;  
END;
```

THRESHOLD MODIFICATION: Modify the value of UN_HEX06 on the RETAIN statement at the beginning of the DATA step that

detects exception conditions for the NLDM VTAM BIND Failure File. In the example below, the value of the threshold for UN_HEX06 has been changed from its original value of 5 to a new value of 10:

```
/* SET ALL THE THRESHOLDS FOR THE UNBIND CODES HERE */  
RETAIN  
UN_HEX06 10 /* INVALID SESSION PARAMETERS */;
```

12853: Virtual Route Inoperative Threshold Exceeded

FILE: NLDM VTAM BIND Failure
SAS FILE NAME: DAYS.NVSVBF01
SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies the hours that have exceeded installation-defined thresholds for the number of UNBIND failures due to a "Virtual Route Inoperative" condition.

RATIONALE: An abnormal UNBIND is a disruptive termination of a terminal user's session with the host application. A large number of UNBINDs indicates problems with either the application or the network components used to access the application. An abnormal UNBIND can occur any time except normal session end, or when one application is passing a terminal session to another application.

DEFINITION: The exception condition is met when the number of failures exceeds installation-defined thresholds.

EXCEPTION STATEMENTS: The SAS statements that identify this exception condition are stored in the member indicated in SOURCE LOCATION and are described below:

```
/* *****  
/* EX NR: 12853  
/* TITLE: VIRTUAL ROUTE INOPERATIVE THRESHOLD EXCEEDED */  
/* FILE: DAYS.NVSVBF01  
/* *****
```

```
IF VBFRCODE='07' AND VBFNRBF GT UN_HEX07 THEN DO;  
  ID =SLU;  
  EXCCODE='12853'; SEVERITY='I'; MGMTAREA='SERVICE';  
  EXCDISC1=  
    'VIRTUAL ROUTE INOPERATIVE THRESHOLD EXCEEDED.';  
  EXCDISC2='PLU/SLU= ' || PLU || '/' || SLU ||  
    ', THRESHOLD= ' || PUT(UN_HEX07,COMMA6.) ||  
    ', NUMBER FOUND= ' || PUT(VBFNRBF,COMMA6.) ;  
  LINK HIT;  
END;
```

THRESHOLD MODIFICATION: Modify the value of UN_HEX07 on the RETAIN statement at the beginning of the DATA step that detects exception conditions for the NLDM VTAM BIND Failure File. In the example below, the value of the threshold for

UN_HEX07 has been changed from its original value of 5 to a new value of 10:

```
/* SET ALL THE THRESHOLDS FOR THE UNBIND CODES HERE */  
RETAIN  
UN_HEX07 10 /* VIRTUAL ROUTE INOPERATIVE */;
```

12854: Route Extension Inoperative Threshold Exceeded

FILE: NLDM VTAM BIND Failure
SAS FILE NAME: DAYS.NVSVBF01
SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies the hours that have exceeded installation-defined thresholds for the number of UNBIND failures due to a "Route Extension Inoperative" condition.

RATIONALE: An abnormal UNBIND is a disruptive termination of a terminal user's session with the host application. A large number of UNBINDs indicates problems with either the application or the network components used to access the application. An abnormal UNBIND can occur any time except normal session end, or when one application is passing a terminal session to another application.

DEFINITION: The exception condition is met when the number of failures exceeds installation-defined thresholds.

EXCEPTION STATEMENTS: The SAS statements that identify this exception condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* *****  
/* EX NR: 12854  
/* TITLE: ROUTE EXTENSION INOPERATIVE THRESHOLD  
/* EXCEEDED.  
/* FILE: DAYS.NVSVBF01  
/* *****
```

```
IF VBFRCODE='08' AND VBFNRBF GT UN_HEX08 THEN DO;  
  ID =SLU;  
  EXCCODE='12854'; SEVERITY='I'; MGMTAREA='SERVICE';  
  EXCDDESC1=  
    'ROUTE EXTENSION INOPERATIVE THRESHOLD EXCEEDED.';  
  EXCDDESC2='PLU/SLU= ' || PLU || '/' || SLU ||  
    ', THRESHOLD= ' || PUT(UN_HEX08,COMMA6.) ||  
    ', NUMBER FOUND= ' || PUT(VBFNRBF,COMMA6.) ;  
  LINK HIT;  
END;
```

THRESHOLD MODIFICATION: Modify the value of UN_HEX08 on the RETAIN statement at the beginning of the DATA step that detects exception conditions for the NDLM VTAM BIND Failure

File. In the example below, the value of the threshold for UN_HEX08 has been changed from its original value of 5 to a new value of 10:

```
/* SET ALL THE THRESHOLDS FOR THE UNBIND CODES HERE */  
RETAIN  
UN_HEX08 10 /* ROUTE EXTENSION INOPERATIVE */;
```

12855: Hierarchical Reset Threshold Exceeded

FILE: NLDM VTAM BIND Failure
SAS FILE NAME: DAYS.NVSVBF01
SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies the hours that have exceeded installation-defined thresholds for the number of UNBIND failures due to a "Hierarchical Reset" condition.

RATIONALE: An abnormal UNBIND is a disruptive termination of a terminal user's session with the host application. A large number of UNBINDs indicates problems with either the application or the network components used to access the application. An abnormal UNBIND can occur any time except normal session end, or when one application is passing a terminal session to another application.

DEFINITION: The exception condition is met when the number of failures exceeds installation-defined thresholds.

EXCEPTION STATEMENTS: The SAS statements that identify this exception condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* *****  
/* EX NR: 12855  
/* TITLE: HIERARCHICAL RESET THRESHOLD EXCEEDED  
/* FILE: DAYS.NVSVBF01  
/* *****  
  
IF VBFRCODE='09' AND VBFNRBF GT UN_HEX09 THEN DO;  
  ID =SLU;  
  EXCCODE='12855'; SEVERITY='I'; MGMTAREA='SERVICE';  
  EXCDISC1=  
    'HIERARCHICAL RESET THRESHOLD EXCEEDED.';  
  EXCDISC2='PLU/SLU= ' || PLU || '/' || SLU ||  
    ', THRESHOLD= ' || PUT(UN_HEX09,COMMA6.) ||  
    ', NUMBER FOUND= ' || PUT(VBFNRBF,COMMA6.) ;  
  LINK HIT;  
END;
```

THRESHOLD MODIFICATION: Modify the value of UN_HEX09 on the RETAIN statement at the beginning of the DATA step that detects exception conditions for the NLDM VTAM BIND Failure File. In the example below, the value of the threshold for

UN_HEX09 has been changed from its original value of 5 to a new value of 10:

```
/* SET ALL THE THRESHOLDS FOR THE UNBIND CODES HERE */  
RETAIN  
UN_HEX09 10 /* HIERARCHAL RESET */;
```

12856: SSCP Gone Threshold Exceeded

FILE: NLDM VTAM BIND Failure
SAS FILE NAME: DAYS.NVSVBF01
SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies the hours that have exceeded installation-defined thresholds for the number of UNBIND failures due to an "SSCP Gone" condition.

RATIONALE: An abnormal UNBIND is a disruptive termination of a terminal user's session with the host application. A large number of UNBINDs indicates problems with either the application or the network components used to access the application. An abnormal UNBIND can occur any time except normal session end, or when one application is passing a terminal session to another application.

DEFINITION: The exception condition is met when the number of failures exceeds installation-defined thresholds.

EXCEPTION STATEMENTS: The SAS statements that identify this exception condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* *****  
/* EX NR: 12856  
/* TITLE: SSCP GONE THRESHOLD EXCEEDED  
/* FILE: DAYS.NVSVBF01  
/* *****  
  
IF VBFRCODE='0A' AND VBFNRBF GT UN_HEX0A THEN DO;  
  ID =SLU;  
  EXCCODE='12856'; SEVERITY='I'; MGMTAREA='SERVICE';  
  EXCDISC1=  
    'SSCP GONE THRESHOLD EXCEEDED.';  
  EXCDISC2='PLU/SLU= ' || PLU || '/' || SLU ||  
    ', THRESHOLD= ' || PUT(UN_HEX0A,COMMA6.) ||  
    ', NUMBER FOUND= ' || PUT(VBFNRBF,COMMA6.) ;  
  LINK HIT;  
END;
```

THRESHOLD MODIFICATION: Modify the value of UN_HEX0A on the RETAIN statement at the beginning of the DATA step that detects exception conditions for the NLDM VTAM BIND Failure

File. In the example below, the value of the threshold for UN_HEX0A has been changed from its original value of 5 to a new value of 10:

```
/* SET ALL THE THRESHOLDS FOR THE UNBIND CODES HERE */  
RETAIN  
UN_HEX0A 10 /* SSCP GONE */;
```

12857: Virtual Route Deactivated Threshold Exceeded

FILE: NLDM VTAM BIND Failure
SAS FILE NAME: DAYS.NVSVBF01
SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies the hours that have exceeded installation-defined thresholds for the number of UNBIND failures due to a "Virtual Route Deactivated" condition.

RATIONALE: An abnormal UNBIND is a disruptive termination of a terminal user's session with the host application. A large number of UNBINDs indicates problems with either the application or the network components used to access the application. An abnormal UNBIND can occur any time except normal session end, or when one application is passing a terminal session to another application.

DEFINITION: The exception condition is met when the number of failures exceeds installation-defined thresholds.

EXCEPTION STATEMENTS: The SAS statements that identify this exception condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* *****  
/* EX NR: 12857  
/* TITLE: VIRTUAL ROUTE DEACTIVATED THRESHOLD EXCEEDED */  
/* FILE: DAYS.NVSVBF01  
/* *****
```

```
IF VBFRCODE='0B' AND VBFNRBF GT UN_HEX0B THEN DO;  
ID =SLU;  
EXCCODE='12857'; SEVERITY='I'; MGMTAREA='SERVICE';  
EXCDESC1=  
    'VIRTUAL ROUTE DEACTIVATED THRESHOLD EXCEEDED.';  
EXCDESC2='PLU/SLU= ' || PLU || '/' || SLU ||  
    ', THRESHOLD= ' || PUT(UN_HEX0B,COMMA6.) ||  
    ', NUMBER FOUND= ' || PUT(VBFNRBF,COMMA6.) ;  
LINK HIT;  
END;
```

THRESHOLD MODIFICATION: Modify the value of UN_HEX0B on the RETAIN statement at the beginning of the DATA step that detects exception conditions for the NLDM VTAM BIND Failure

File. In the example below, the value of the threshold for UN_HEX0B has been changed from its original value of 5 to a new value of 10:

```
/* SET ALL THE THRESHOLDS FOR THE UNBIND CODES HERE */  
RETAIN  
UN_HEX0B 10 /* VIRTUAL ROUTE DEACTIVATED */;
```

12858: LU Failure - Unrecoverable Threshold Exceeded

FILE: NLDM VTAM BIND Failure
SAS FILE NAME: DAYS.NVSVBF01
SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies the hours that have exceeded installation-defined thresholds for the number of UNBIND failures due to a "LU Failure - Unrecoverable" condition.

RATIONALE: An abnormal UNBIND is a disruptive termination of a terminal user's session with the host application. A large number of UNBINDs indicates problems with either the application or the network components used to access the application. An abnormal UNBIND can occur any time except normal session end, or when one application is passing a terminal session to another application.

DEFINITION: The exception condition is met when the number of failures exceeds installation-defined thresholds.

EXCEPTION STATEMENTS: The SAS statements that identify this exception condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* *****  
/* EX NR: 12858  
/* TITLE: LU FAILURE - UNRECOVERABLE THRESHOLD EXCEEDED */  
/* FILE: DAYS.NVSVBF01  
/* *****
```

```
IF VBFRCODE='0C' AND VBFNRBF GT UN_HEX0C THEN DO;  
ID =SLU;  
EXCCODE='12858'; SEVERITY='I'; MGMTAREA='SERVICE';  
EXCDESC1=  
    'LU FAILURE - UNRECOVERABLE THRESHOLD EXCEEDED.';  
EXCDESC2='PLU/SLU= ' || PLU || '/' || SLU ||  
    ', THRESHOLD= ' || PUT(UN_HEX0C,COMMA6.) ||  
    ', NUMBER FOUND= ' || PUT(VBFNRBF,COMMA6.) ;  
LINK HIT;  
END;
```

THRESHOLD MODIFICATION: Modify the value of UN_HEX0C on the RETAIN statement at the beginning of the DATA step that detects exception conditions for the NLDM VTAM BIND Failure File. In the example below, the value of the threshold for

UN_HEX0C has been changed from its original value of 5 to a new value of 10:

```
/* SET ALL THE THRESHOLDS FOR THE UNBIND CODES HERE */  
RETAIN  
UN_HEX0C 10 /* LU FAILURE UNRECOVERABLE */;
```

12859: LU Failure - Recoverable Threshold Exceeded

FILE: NLDM VTAM BIND Failure
SAS FILE NAME: DAYS.NVSVBF01
SOURCE LOCATION: prefix.MICS.USER.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies the hours that have exceeded installation-defined thresholds for the number of UNBIND failures due to a "LU Failure - Recoverable" condition.

RATIONALE: An abnormal UNBIND is a disruptive termination of a terminal user's session with the host application. A large number of UNBINDs indicates problems with either the application or the network components used to access the application. An abnormal UNBIND can occur any time except normal session end, or when one application is passing a terminal session to another application.

DEFINITION: The exception condition is met when the number of failures exceeds installation-defined thresholds.

EXCEPTION STATEMENTS: The SAS statements that identify this exception condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* *****/
/* EX NR: 12859 */
/* TITLE: LU FAILURE - RECOVERABLE THRESHOLD EXCEEDED */
/* FILE: DAYS.NVSVBF01 */
/* *****/

IF VBFRCODE='0E' AND VBFNRBF GT UN_HEX0E THEN DO;
  ID =SLU;
  EXCCODE='12859'; SEVERITY='I'; MGMTAREA='SERVICE';
  EXCDISC1=
    'LU FAILURE - RECOVERABLE THRESHOLD EXCEEDED.';
  EXCDISC2='PLU/SLU= ' || PLU || '/' || SLU ||
    ', THRESHOLD= ' || PUT(UN_HEX0E,COMMA6.) ||
    ', NUMBER FOUND= ' || PUT(VBFNRBF,COMMA6.) ;
  LINK HIT;
END;
```

THRESHOLD MODIFICATION: Modify the value of UN_HEX0E on the RETAIN statement at the beginning of the DATA step that

detects exception conditions for the NLDM VTAM BIND Failure File. In the example below, the value of the threshold for UN_HEX0E has been changed from its original value of 5 to a new value of 10:

```
/* SET ALL THE THRESHOLDS FOR THE UNBIND CODES HERE */  
RETAIN  
UN_HEX0E 10 /* LU FAILURE - RECOVERABLE */;
```

12862: Session Failure Threshold Exceeded

FILE: NLDM VTAM BIND Failure
SAS FILE NAME: DAYS.NVSVBF01
SOURCE LOCATION: sharedprefix.MICS.SOURCE(DYSNTEXC)

SEVERITY: Impacting (SEVERITY='I')
MANAGEMENT AREA: Service (MGMTAREA='SERVICE')

PURPOSE: Identifies the hours that have exceeded installation-defined thresholds for the number of UNBIND failures due to a "Session Failure" condition.

RATIONALE: An abnormal UNBIND is a disruptive termination of a terminal user's session with the host application. A large number of UNBINDs indicates problems with either the application or the network components used to access the application. An abnormal UNBIND can occur any time except normal session end, or when one application is passing a terminal session to another application.

DEFINITION: The exception condition is met when the number of failures exceeds installation-defined thresholds.

EXCEPTION STATEMENTS: The SAS statements that identify this exception condition are stored in the source member named in SOURCE LOCATION and are described below:

```
/* *****  
/* EX NR: 12862  
/* TITLE: SESSION FAILURE THRESHOLD EXCEEDED  
/* FILE: DAYS.NVSVBF01  
/* *****  
  
IF VBFRCODE='FE' AND VBFNRBF GT UN_HEXFE THEN DO;  
  ID =SLU;  
  EXCCODE='12862'; SEVERITY='I'; MGMTAREA='SERVICE';  
  EXCDISC1=  
    'SESSION FAILURE THRESHOLD EXCEEDED.';  
  EXCDISC2='PLU/SLU= ' || PLU || '/' || SLU ||  
    ', THRESHOLD= ' || PUT(UN_HEXFE,COMMA6.) ||  
    ', NUMBER FOUND= ' || PUT(VBFNRBF,COMMA6.) ;  
  LINK HIT;  
END
```

THRESHOLD MODIFICATION: Modify the value of UN_HEXFE on the RETAIN statement at the beginning of the DATA step that detects exception conditions for the NLDM VTAM BIND Failure

File. In the example below, the value of the threshold for UN_HEXFE has been changed from its original value of 5 to a new value of 10:

```
/* SET ALL THE THRESHOLDS FOR THE UNBIND CODES HERE */
RETAIN
UN_HEXFE 10 /* SESSION FAILURE */;
```


Chapter 5: DATABASE FILES

This chapter describes the database files supported by the CA MICS Network Analyzer Option. It includes detailed data element lists, timespan granularity charts, usage considerations, and retrieval examples for each file.

This section contains the following topics:

[5.1 Data Element Naming Conventions](#) (see page 638)

[5.2 SNT Information Area](#) (see page 639)

[5.3 NVS Information Area](#) (see page 816)

[5.4 TCP Information Area](#) (see page 873)

5.1 Data Element Naming Conventions

There are two types of CA MICS data elements: standard and common. Standard data elements are unique to a CA MICS file, while common data elements are used by more than one file.

The first three characters of a standard data element's name are the three-character file identifiers to which the element belongs.

Common data elements do not use a data element prefix. They have a common definition across database information areas or across files within an information area. Common data elements are listed in the Sequence/Summary Data Elements and Common Data Elements sections of the data elements lists that accompany the following file documentation.

The chart on the next page lists each file's descriptive name, its six-character file name, and the three-character standard data element name prefix.

File Name	File	Names Begin With
NCP Link	SNTNCL	NCL
Network Components Activity	SNTCAF	CAF
NCP Activity	SNTNAF	NAF
Network Incident	SNTNIN	NIN
NPM User Activity	SNTPSU	PSU
NPM System (PLU) Activity	SNTPSY	PSY
NCP Line Processor Activity	SNTNLP	NLP
NPM Link Activity	SNTNPL	NPL
CA NetSpy Application (PLU)	SNTNSP	NSP
CA NetSpy Terminal (SLU)	SNTNSS	NSS
CA NetSpy TCP/IP Telnet Server	SNTNTS	NTS
CA NetSpy Virtual Route Act'y	SNTNVR	NVR
NCP Network Accounting	SNTNAC	NAC
NPDA Event	SNTNEF	NEF
NPDA Statistical	SNTNSF	NSF
NPDA LAN	SNTLNF	LNf
NPDA Generic Alert	SNTGAF	GAF
NLDM Service	SNTNSV	NSV
NLDM System (PLU) Activity	NVSLSY	LSY
NLDM Session Accounting	NVSNSA	NSA
NLDM Session Connectivity	NVSNsc	NSC
NLDM Link Activity	NVSNLL	NLL
NLDM Route	NVSRTE	RTE
NLDM Response Time	NVSRtm	RTM
NLDM VTAM Bind Failure	NVSVBF	VBF

Telnet Server File	TCPSTN	STN	
Telnet Client File	TCPCTN	CTN	
FTP Server File	TCPFSF	FSF	
FTP Client File	TCPFCF	FCF	
API Calls for Sockets	TCPAPI	API	
IP Statistics	TCPIPX	IPX	
ICMP Statistics	TCPICX	ICX	
TCP Statistics	TCPTCI	TCI	
UDP Statistics	TCPUDI	UDI	
+-----+-----+-----+			

5.2 SNT Information Area

The SNT Information Area captures information about networks in these files, which are described in this chapter:

- 1 - NCP Link File (SNTNCL)
- 2 - Network Components Activity File (SNTCAF)
- 3 - NCP Activity File (SNTNAF)
- 4 - Network Incident File (SNTNIN)
- 5 - NPM User Activity File (SNTPSU)
- 6 - NPM System (PLU) Activity File (SNTPSY)
- 7 - NPM Link Activity File (SNTNPL)
- 8 - NPDA Event File (SNTNEF)
- 9 - NPDA Statistical File (SNTNSF)
- 10 - NPDA LAN File (SNTLNF)
- 11 - NPDA Generic Alert File (SNTGAF)
- 12 - NLDM Service File (SNTNSV)
- 13 - NetSpy Application (PLU) File (SNTNSP)
- 14 - NetSpy Terminal (SLU) File (SNTNSS)
- 15 - NetSpy Virtual Route Activity File (SNTNVR)
- 16 - NCP Network Accounting File (SNTNAC)
- 17 - NCP Line Processor Activity File (SNTNLP)
- 18 - Telnet Server Entry File (SNTNTS)
- 19 - Stack Entry File (SNTTCS)
- 20 - VTAM Buffer Pool Data File (SNTVBS)
- 21 - VTAM CSM Data File (SNTVCS)
- 22 - VTAM Global Data File (SNTVGB)

5.2.1 NCP Link File (SNTNCL)

The NCP Link File (SNTNCL) contains data that quantifies input and output character traffic, error and retransmit counts for each SDLC or bisync line for which data is recorded, and statistics for NTRI (Network Token-Ring Interface), NPSI (NCP Packet Switching Interface), TIC3 (Token Interface Coupler-3), and Frame Relay environments.

The file is derived from NPM or CA NetSpy running on z/OS or VM systems.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.1.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	NCPNAME	NETNAME	YEAR	
	MONTH	DAY	HOUR	ENDTS		
DAYS	NETWRKID	SYSID	NCPNAME	NETNAME	YEAR	
	MONTH	DAY	HOUR			
WEEKS	NETWRKID	SYSID	NCPNAME	NETNAME	YEAR	
	WEEK	ZONE	HOUR			
MONTHS	NETWRKID	SYSID	NCPNAME	NETNAME	YEAR	
	MONTH	ZONE				
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=DEFAult option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-1. SNTNCL Timespan Granularity Chart

5.2.1.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD....E	DAY	- Day of Month
XDW...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWM..E	NCPNAME	- Network Ctl Program Name
XDWM..E	NETNAME	- Resource Network Name
XDWM..E	NETWKID	- Network Identifier
XDWM..E	SYSID	- System Identifier
XDW...E	WEEK	- Week of Year
XDWM..E	YEAR	- Year of Century
XDWM..E	ZONE	- Time Zone

Common Data Elements

XDWM..E	DATATYPE	- Type of Data Contained in Observation
XD....E	DAYNAME	- Name of Day of Week
XDWM..E	DURATION	- Recording Interval Time
XDWM..E	ENDTS	- End Time Stamp
XDWM..E	INTERVLS	- Number of Recording Intervals
XDWM..	LINKSPD	- Link Speed
XDWM..	LNKTPCID	- Network Link TP Circuit Id
XDWM..	MICSVER	- CA MICS Version Number
X.....E	NPMIPADR	- NPM IP Address
XDWM..	NPMTMAOT	- Actual Observation Time
XDWM..	NPMTSEIS	- Expected Interval Time
XDWM..	NPMTSFRU	- Forward RU Send Time
XDWM..	NPMTSLOG	- Time Record Logged To SMF
XDWM..E	NTRIDATA	- NTRI Data Physical/Logical (P or L)
XDWM..E	NTRILINK	- NTRI Link Yes/No (Y or N)
XDWM..E	PLUNETID	- PLU Network Id
XDWM..	PRODUCT	- Network Product (Source) Name
XDWM..E	PRODVRL	- Product Version and Release
XDWM..	RESNAME	- Resource Generic Name
XDWM..E	STARTTS	- Start Time Stamp
XDWM..	TMOFFSET	- Time Offset

Retained Data Elements

XDM..E NCLHPRBR - Number of HPR Bytes Received
XDM..E NCLHPRBS - Number of HPR Bytes Sent
XDM..E NCLHPRCD - Number of HPR Frames Discarded - CiN
XDM..E NCLHPRFR - Number of HPR Frames Received
XDM..E NCLHPRFS - Number of HPR Frames Sent
XDM..E NCLHPROQ - Number of HPR Bytes Queued for Xmit
XDM..E NCLHPRXD - Number of HPR Frames Discarded - XTQT
XDM..E NCLNRRLS - Receiving Link Speed
XDM..E NCLNRSLS - Sending Link Speed
XDM..E NCLNRTMR - Timer
XDM..E NCLPFRTM - Time Per Frame Received (Microseconds)
XDM..E NCLPFSTM - Time Per Frame Sent (Microseconds)
XDM..E NCLPNRTM - Time Per Byte Received (Nanoseconds)
XDM..E NCLPNSTM - Time Per Byte Sent (Nanoseconds)
XDM..E NCLVSWPU - VTAM Switch Physical Unit

Accumulated Data Elements

XDM.. NCLIDITM - Idle Interval Time
XDM..E NCLNRALC - Active Logical Connections
XDM..E NCLNRBWC - Number Backward Congestion Count
XDM..E NCLNRCHR - Number Of Bytes Received
XDM..E NCLNRCHS - Number Of Bytes Sent
XDM..E NCLNRCON - Congestion Count
XDM..E NCLNRDFR - Number of Frames Discarded
XDM..E NCLNRERR - Error Count
XDM..E NCLNRFRR - Number of Frames Received
XDM..E NCLNRFRS - Number of Frames Sent
XDM..E NCLNRFWC - Number Forward Congestion Count
XDM..E NCLNRIFR - Number of I-Frames Received
XDM..E NCLNRIFS - Number of I-Frames Sent
XDM.. NCLNRMSR - Number Of Messages Received
XDM.. NCLNRMSS - Number Of Messages Sent
XDM.. NCLNRPIU - Retransmit PIU Count
XDM..E NCLNRPPL - Positive Poll Count
XDM..E NCLNRRBY - Retransmit Byte Count
XDM..E NCLNRRFD - Number of Receive Frames Discarded
XDM..E NCLNRRFM - Number of Receive Frames Misaddressed
XDM..E NCLNRRFR - Total RR Frames Received
XDM..E NCLNRRFS - Total RR Frames Sent
XDM..E NCLNRRFU - Number of Receive Frames Unrecognized
XDM..E NCLNRRIF - Retransmit I-Frame Count
XDM..E NCLNRROQ - Resource Outbound Queue Length
XDM..E NCLNRRRR - Total RNR Frames Received
XDM..E NCLNRRRS - Total RNR Frames Sent
XDM..E NCLNRRTO - Reply Time Outs
XDM..E NCLNRTPL - Total Poll Count

Minimum Data Elements

XDW..E NCLMNLBS - Minimum Percent Link Busy
XDW.. NCLMNRLB - Minimum Percent Link Busy Receiving
XDW.. NCLMNSLB - Minimum Percent Link Busy Sending

Maximum Data Elements

XDW..E NCLMXLBS - Maximum Percent Link Busy
XDW.. NCLMXRLB - Maximum Percent Link Busy Receiving
XDW..E NCLMXROQ - Maximum Resource Outbound Q Length
XDW.. NCLMXSLB - Maximum Percent Link Busy Sending

Derived Data Elements

XDW.. NCLNRNPL - Negative Poll Count
XDW..E NCLPCELB - Percent Link Busy Retransmission
XDW..E NCLPCLBS - Percent Link (Line) Busy
XDW.. NCLPCRLB - Percent Link Busy Receiving
XDW.. NCLPCSLB - Percent Link Busy Sending
XDW.. NCLPMCHR - Number of Bytes Received per Minute
XDW.. NCLPMCHS - Number of Bytes Sent per Minute
XDW.. NCLPMIFR - Number of I-Frames Received per Minute
XDW.. NCLPMIFS - Number of I-Frames Sent per Minute
XDW.. NCLPMSR - Number of Messages Received per Minute
XDW.. NCLPMSS - Number of Messages Sent per Minute
XDW..E NCLPMTPL - Number of (Total) Polls per Minute

5.2.1.3 Usage Considerations

This section identifies the special considerations or techniques related to using the SNTNCL file, followed by several retrieval examples.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &ddiit, where d is the database identifier, iit is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Exercise care in using the special date and time data elements contained in each CA MICS file. As the file's granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEK should not be used in MONTHS.
2. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7. For NPM, NETWRKID may be set to the value of PLU Network Identifier (PLUNETID).
 - o LNKTPCID - Link TP Circuit ID value. This data element will typically contain the value of the link vendor's (AT&T, MCI, etc.) billing identifier. It is set in the Link TP Circuit ID Exit Routine, SNTCIDRT, discussed in Chapter 7.
 - o TMOFFSET - Time offset applied to the data in the file. The user can associate a time offset with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is

brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. Time offset is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

3. The following data elements lose significance once summarization has been performed. You should reference these data elements only when the last observed value in a summarization interval is significant.

- LINKSPD - Link Speed
- NPMTSFRU - Forward RU Send Time
- NPMTSLOG - Time Record Logged to SMF
- NPMTSEIS - Expected Interval Time
- NCLNRRLS - Receiving Link Speed
- NCLNRSLS - Sending Link Speed

4. If the data source for this file is the CA NetSpy SMF Record, then the following element will have missing values:

- o NPMTSFRU - Forward RU Send Time

5. The CA MICS Network Analyzer Option makes the following assumptions and calculations regarding link speed data elements:

- o The values coded for sending and receiving line speeds in NCP generations are generally for documentation purposes only; however, the majority of data centers code a value for sending line speed. The typical exception to this "rule" is for full duplex lines, where NCP parameters for both sending and receiving line speeds may be appropriate.

Note: Line speeds are required for those devices (for example, modems) that use external clocking.

- o LINKSPD - In the case of full duplex lines where both sending and receiving line speeds may be coded, LINKSPD will be the maximum of both line speeds. For half duplex lines, it will be the primary line speed.
- o NCLPCELB (Percent Link Busy Retransmission) - sending line speed used if greater than zero, else set to missing.
- o NCLPCLBS (Percent Link Busy) - LINKSPD used if greater

than zero, else set to missing.

- o NCLPCRLB (Percent Link Busy Receiving) - receiving line speed used if coded in NCP gen; if receiving speed is zero, sending speed is used if it is greater than zero (else set to missing).
- o NCLPCSLB (Percent Link Busy Sending) - sending line speed used if greater than zero, else set to missing.

6. The values of the following elements include retransmitted bytes:

- o NCLPCLBS (Percent Link Busy)
- o NCLPCRLB (Percent Link Busy Receiving)
- o NCLPCSLB (Percent Link Busy Sending)
- o NCLNRCHR (Number of Bytes Received)
- o NCLNRCHS (Number of Bytes Sent)
- o NCLNRIFR (Number of I-Frames Received)
- o NCLNRIFS (Number of I-Frames Sent)

That the above elements include retransmitted bytes is a feature of how the NCP NPA logical unit measures bytes sent and received, not a feature of CA MICS.

That the above elements include retransmitted bytes is an important consideration, if, for example, you are creating a stacked vertical bar chart of Percent Link Busy and Percent Link Busy Retransmission. Unless you subtract the latter measurement from the former one, the resulting total percentage may be greater than 100.

Retrieval Examples

1. To produce a chart depicting the percent of line busy during the peak hour for the last five days:

```
DATA SELFIE;  
  SET &PSNTD..SNTNCL01 &PSNTD..SNTNCL02 &PSNTD..SNTNCL03  
    &PSNTD..SNTNCL04 &PSNTD..SNTNCL05;  
  IF HOUR=14 AND NETNAME='LN001003';
```

```
PROC CHART DATA=SELFIE;  
  VBAR DAYNAME / SUMVAR=NCLPCLBS;
```

2. To produce a report depicting the 25 lines having the highest count of retransmitted bytes yesterday:

```
%LET BY = NETWKID SYSID NETNAME ;
```



```
%LET BREAK = NETNAME ;

PROC SORT DATA=&PSNTD..SNTNCL01 OUT=WKNCL;
  BY &BY;

DATA WKNCL;
  SET WKNCL;
  %NCLSUM;

PROC SORT DATA=WKNCL;
  BY DESCENDING NCLNRRBY;

OPTIONS OBS=25;
PROC PRINT DATA=WKNCL;
  ID NETNAME;
  VAR SYSID NCLNRRBY;
```

5.2.2 Network Components Activity File (SNTCAF)

The Network Components Activity File (SNTCAF) contains data that quantifies input and output character traffic, error and retransmit counts, polling statistics for SDLC physical and logical units, BISYNC clusters and terminals, x.25 machine physical units, virtual circuits, LUs, TIC3 physical units, and other network components for which data is recorded.

This file is derived from NPM and CA NetSpy running on z/OS or VM systems.

Data from SDLC links, BISYNC links, X.25 links, NTRI links, and TIC3 links is included in the SNTNCL (NCP Link) file and therefore excluded from this file. Data about 37xx NCP activity is included in the SNTNAF (NCP Activity) file and therefore excluded from this file.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.2.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	N/A					
DAYS	NETWRKID	SYSID	NCPNAME	NETNAME	YEAR	
	MONTH	DAY	HOUR			
WEEKS	NETWRKID	SYSID	NCPNAME	NETNAME	YEAR	
	WEEK	ZONE	HOUR			
MONTHS	NETWRKID	SYSID	NCPNAME	NETNAME	YEAR	
	MONTH	ZONE				
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=DEFAult option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-2. SNTCAF Timespan Granularity Chart

5.2.2.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

.D...E	DAY	- Day of Month
.DW...E	HOURL	- Hour of Day
.D.M..E	MONTH	- Month of Year
.DWM..E	NCPNAME	- Network Ctl Program Name
.DWM..E	NETNAME	- Resource Network Name
.DWM..E	NETWKID	- Network Identifier

.DWM..E SYSID - System Identifier
 .DW...E WEEK - Week of Year
 .DWM..E YEAR - Year of Century
 .DWM..E ZONE - Time Zone

Common Data Elements

.DWM..E DATATYPE - Type of Data Contained in Observation
 .D....E DAYNAME - Name of Day of Week
 .DWM.. DURATION - Recording Interval Time
 .DWM..E ENDTS - End Time Stamp
 .DWM..E INTERVLS - Number of Recording Intervals
 .DWM.. MICSVER - CA MICS Version Number
E NPMIPADR - NPM IP Address
 .DWM.. NPMTMAOT - Actual Observation Time
 .DWM.. NPMTSEIS - Expected Interval Time
 .DWM.. NPMTSFRU - Forward RU Send Time
 .DWM.. NPMTSLOG - Time Record Logged To SMF
 .DWM..E NPMVRL - NPM Version/Release Number
 .DWM..E PLUNETID - PLU Network Id
 .DWM.. PRODUCT - Network Product (Source) Name
 .DWM.. RESNAME - Resource Generic Name
 .DWM..E STARTTS - Start Time Stamp
 .DWM.. TMOFFSET - Time Offset

Retained Data Elements

.DWM..E CAFHPRBR - Number of HPR Bytes Received
 .DWM..E CAFHPRBS - Number of HPR Bytes Sent
 .DWM..E CAFHPRCD - Number of HPR Frames Discarded - CiN
 .DWM..E CAFHPRFR - Number of HPR Frames Received
 .DWM..E CAFHPRFS - Number of HPR Frames Sent
 .DWM..E CAFHPROQ - Number of HPR Bytes Queued for Xmit
 .DWM..E CAFHPRXD - Number of HPR Frames Discarded - XTQT
 .DWM..E CAFNRRLS - Receiving Link Speed
 .DWM..E CAFNRSLs - Sending Link Speed
 .DWM..E CAFNRTMR - Timer
 .DWM..E CAFVSWPU - VTAM Switch Physical Unit

Accumulated Data Elements

.DWM.. CAFIDITM - Idle Interval Time
 .DWM..E CAFNRBWC - Number Backward Congestion Count
 .DWM.. CAFNRCHR - Number Of Bytes Received
 .DWM.. CAFNRCHS - Number Of Bytes Sent
 .DWM..E CAFNRCVC - Total VCs Connected at Interval End
 .DWM..E CAFNRDFR - Number of Frames Discarded
 .DWM..E CAFNRDPR - Total D-Bit Packets Received
 .DWM..E CAFNRDPS - Total D-Bit Packets Sent

.DWM..E CAFNRERR - Error Count
.DWM..E CAFNRFRR - Number of Frames Received
.DWM..E CAFNRFRRS - Number of Frames Sent
.DWM..E CAFNRFWC - Number Forward Congestion Count
.DWM..E CAFNRIBC - Total Inbound Connections
.DWM..E CAFNRIBD - Total Inbound Disconnections
.DWM..E CAFNRIFR - Number of I-Frames Received
.DWM..E CAFNRIFS - Number of I-Frames Sent
.DWM..E CAFNRISR - Total INN-SHM Reconnections
.DWM..E CAFNRIVC - New VCs During Interval
.DWM..E CAFNRLBO - Local Busy Occurrences
.DWM..E CAFNRMPPR - Total M-Bit Packets Received
.DWM..E CAFNRMPS - Total M-Bit Packets Sent
.DWM.. CAFNRMSR - Number Of Messages Received
.DWM.. CAFNRMSS - Number Of Messages Sent
.DWM..E CAFNROBC - Total Outbound Connections
.DWM..E CAFNROBD - Total Outbound Disconnections
.DWM.. CAFNRPIU - Retransmit PIU Count
.DWM..E CAFNRPKR - Total Packets Received
.DWM..E CAFNRPKS - Total Packets Sent
.DWM.. CAFNRPPL - Positive Poll Count
.DWM.. CAFNRRBY - Retransmit Byte Count
.DWM..E CAFNRRIF - Retransmitted I-Frame Count
.DWM..E CAFNRRQ - Resource Outbound Queue Length
.DWM..E CAFNRRRR - Total RNR Frames Received
.DWM..E CAFNRRRS - Total RNR Frames Sent
.DWM..E CAFNRRT0 - Reply Timeouts
.DWM..E CAFNRSFR - Rejected Supervisor Frames Received
.DWM..E CAFNRSFS - Rejected Supervisor Frames Sent
.DWM.. CAFNRTPL - Total Poll Count

Maximum Data Elements

.DWM..E CAFMXRQ - Maximum Resource Outbound Q Length

Derived Data Elements

.DWM.. CAFNRNPL - Negative Poll Count
.DWM.. CAFPMCHR - Number of Bytes Received per Minute
.DWM.. CAFPMCHS - Number of Bytes Sent per Minute
.DWM.. CAFPMMSR - Number of Messages Received per Minute
.DWM.. CAFPMSS - Number of Messages Sent per Minute
.DWM.. CAFPMPKR - Number of Packets Received per Minute
.DWM.. CAFPMPKS - Number of Packets Sent per Minute
.DWM.. CAFPMTPL - Number of (Total) Polls per Minute

5.2.2.3 Usage Considerations

This section identifies the special considerations or techniques related to using the SNTCAF file, followed by several retrieval examples.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As the file's granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEK should not be used in MONTHS.
2. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7. For NPM, NETWRKID may be set to the value of PLU Network Identifier (PLUNETID).
 - o TMOFFSET - Time offset applied to the data in the file. The user can associate a time offset with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. Time offset is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

3. The following data elements lose significance once summarization has been performed. These data elements should be referenced only when the last observed value in a summarization interval is significant.

NPMTSFRU - Forward RU Send Time
NPMTSLOG - Time Record Logged to SMF
NPMTSEIS - Expected Interval Time

4. If the data source for this file is the CA NetSpy SMF Record, then the following element will have missing values:

o NPMTSFRU - Forward RU Send Time

Retrieval Example

Produce a chart showing the error occurrences for each network component for the month to date:

```
PROC CHART DATA=&PSNTM..SNTCAF00;  
  HBAR NETNAME / SUMVAR=CAFNERRR DESCENDING;
```

5.2.3 NCP Activity File (SNTNAF)

The NCP Activity File contains data that quantifies CCU cycle and buffer usage for each Network Control Program operating in a communications controller (37xx). This data is only recorded for NCPs for which data is recorded in NPM or CA NetSpy SMF records or their VM equivalents.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.3.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	NCPNAME	YEAR	MONTH	
	DAY	HOUR	ENDTS			
DAYS	NETWRKID	SYSID	NCPNAME	YEAR	MONTH	
	DAY	HOUR				
WEEKS	NETWRKID	SYSID	NCPNAME	YEAR	WEEK	
	ZONE	HOUR				
MONTHS	NETWRKID	SYSID	NCPNAME	YEAR	MONTH	
	ZONE					
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=DEFAult option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-3. SNTNAF Timespan Granularity Chart

5.2.3.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

X - DETAIL
 D - DAYS
 W - WEEKS
 M - MONTHS
 Y - YEARS
 T - TABLES AREA
 . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XDW...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWM..E	NCPNAME	- Network Ctl Program Name
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	SYSID	- System Identifier

XDW...E WEEK - Week of Year
XDW..E YEAR - Year of Century
XDW..E ZONE - Time Zone

Common Data Elements

XDW..E DATATYPE - Type of Data Contained in Observation
XD....E DAYNAME - Name of Day of Week
XDW..E DURATION - Recording Interval Time
XDW..E ENDTS - End Time Stamp
XDW..E INTERVLS - Number of Recording Intervals
XDW.. MICSVER - CA MICS Version Number
XDW.. NETNAME - Resource Network Name
X.....E NPMIPADR - NPM IP Address
XDW..E NPMTMAOT - Actual Observation Time
XDW.. NPMTSEIS - Expected Interval Time
XDW.. NPMTSFRU - Forward RU Send Time
XDW.. NPMTSLOG - Time Record Logged To SMF
XDW..E NPMVRL - NPM Version/Release Number
XDW..E PLUNETID - PLU Network Id
XDW..E PRODUCT - Network Product (Source) Name
XDW.. RESNAME - Resource Generic Name
XDW..E STARTTS - Start Time Stamp
XDW.. TMOFFSET - Time Offset

Retained Data Elements

XDW..E NAFCCUSP - CCU Cycle Speed / 80 (NetSpy only)

Accumulated Data Elements

XDW..E NAFNRCYC - Number of CCU Cycles Used / 8 (NetSpy)
XDW.. NAFNRDBU - Buffers Used For Dynam Control Blocks
XDW..E NAFNRFBQ - Free Buffer Queue Length
XDW..E NAFNRHQL - NCP Channel Hold Queue Length
XDW.. NAFNRIQL - NCP Channel Intermed. Queue Len.
XDW.. NAFNRSFB - Free Buffer Count At Slowdown
XDW..E NAFTMFCT - Free Cycle Time
XDW..E NAFTMTIS - Time In Slowdown

Minimum Data Elements

XDW..E NAFMNCCU - Minimum Percent CCU Utilization
XDW.. NAFMNFBL - Free Buffer Low Water Mark
XDW.. NAFMNFBU - Minimum Free Buffer Queue Length
XDW.. NAFMNHQL - Minimum Channel Hold Queue Length
XDW.. NAFMNIQL - Minimum Channel Intermed. Queue Len.
XDW..E NAFMNNBU - Minimum Percent NCP Buffer Utilization
XDW.. NAFMNSFB - Minimum Free Buffer Count At Slowdown

Maximum Data Elements

XDW..E NAFMXANP - Max Available NCP Buffers
XDW..E NAFMXCCU - Maximum Percent CCU Utilization
XDW.. NAFMXDBA - Max Buf Avail For Dynam Control Blocks
XDW.. NAFMXDBU - Max Buf used For Dynam Control Blocks
XDW.. NAFMXFBH - Free Buffer High Water Mark
XDW.. NAFMXFBQ - Maximum Free Buffer Queue Length
XDW.. NAFMXHQL - Maximum Channel Hold Queue Length
XDW.. NAFMXIQL - Maximum Channel Intermed. Queue Len.
XDW..E NAFMXNBU - Maximum Percent NCP Buffer Utilization
XDW.. NAFMXSFB - Maximum Free Buffer Count At Slowdown

Derived Data Elements

XDW..E NFAVFBQ - Avg Free Buffer Queue Length
XDW..E NFAVHQL - Avg NCP Channel Hold Queue Length
XDW.. NFAVIQL - Avg NCP Channel Intermed. Queue Len.
XDW.. NFAVSFB - Avg Free Buffer Count At Slowdown
XDW..E NAFPCCU - Percent Communications Controller Util.
XDW..E NAFPCNBU - Percent NCP Buffer Utilization
XDW..E NAFPTIS - Percent Time in Slowdown

5.2.3.3 Usage Considerations

This section identifies the special considerations or techniques related to using the SNTNAF file, followed by several retrieval examples.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As the file's granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEK should not be used in MONTHS.
2. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7. For NPM, NETWRKID may be set to the value of PLU Network Identifier (PLUNETID).
 - o TMOFFSET - Time offset applied to the data in the file. The user can associate a time offset with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. Time offset is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

3. The following data elements lose significance once summarization has been performed. These data elements should be referenced only when the last observed value in a summarization interval is significant.

NPMTSFRU - Forward RU Send Time
NPMTSLOG - Time Record Logged to SMF
NPMTSEIS - Expected Interval Time
NETNAME - Network Name
RESNAME - Resource Generic Name

4. The following accumulated data elements exist above the detail timespan only for the purpose of recomputing their minimum, maximum, or average values at the higher timespans. Do not use these accumulated elements above the detail timespan; instead, refer to the minimum, maximum, or average values that are derived from them.
- o NAFNRFBQ - Free Buffer Queue Length. Above detail, refer to the elements for minimum, maximum, or average free buffer queue length
 - o NAFNRHQL - NCP Channel Hold Queue Length. Above detail, refer to the elements for minimum, maximum or average channel hold queue length
 - o NAFNRIQL - NCP Channel Intermed. Queue Len. Above detail, refer to the elements for minimum, maximum or average channel intermed. queue length
 - o NAFNRSFB - Free Buffer Count At Slowdown. Above detail, refer to the elements for minimum, maximum or average free buffer count at slowdown
5. If the data source for this file is the CA NetSpy SMF Record, then the following element will have missing values:
- o NPMTSFRU--Forward RU Send Time
6. Three elements in this file will have missing values, unless the data source is the CA NetSpy SMF record. The three elements are:
- o NAFCCUSP--CCU Speed
 - o NAFNRCYC--Number of CCU Cycles Used
 - o NAFTMFCT--Free Cycle Time

Retrieval Examples

1. Produce a chart showing the relationship of productive NCP processing time to Free Cycle time and time in slowdown. Use week-to-date data:

```
DATA WKNAF (KEEP=TIME TIMETYPE NCPNAME ZONE HOUR);
SET &PSNTW..SNTNAF00;
  TIME=NAFTMFCT;
  TIMETYPE='FREE TIME';
  OUTPUT;
  TIME=NAFTMTIS;
  TIMETYPE='SLOWDOWN';
  OUTPUT;
  TIME=NPMTMAOT-NAFTMFCT-NAFTMTIS;
  TIMETYPE='PRODUCTIVE';
  OUTPUT;
  RUN;
```

```
PROC CHART DATA= WKNAF;
  VBAR HOUR / SUBGROUP=TIMETYPE
    SUMVAR=TIME
    DISCRETE;RUN;
```

2. Produce a chart showing 37xx free cycle time by hour, using yesterday's data:

```
PROC CHART DATA=&PSNTD..SNTNAF01;
  VBAR HOUR / SUBGROUP=NCPNAME
    SUMVAR=NAFTMFCT
    DISCRETE;RUN;
```


5.2.4 Network Incident File (SNTNIN)

The Network Incident File (SNTNIN) contains data that identifies problems in the operation, performance, and integrity of the network from the perspective of the Network Control Program (NCP). The file is derived from either CA NetSpy or NPM SMF records or their VM equivalents.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.4.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	NINCODE	YEAR	MONTH	
	DAY	HOUR	ENDTS			
DAYS	N/A					
WEEKS	N/A					
MONTHS	NETWRKID	SYSID	NINCODE	YEAR	MONTH	
	ZONE					
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-4. SNTNIN Timespan Granularity Chart

5.2.4.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

X - DETAIL
 D - DAYS
 W - WEEKS
 M - MONTHS
 Y - YEARS
 T - TABLES AREA
 . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

X....E	DAY	- Day of Month
X....E	HOURL	- Hour of Day
X..M..E	MONTH	- Month of Year
X..M..E	NETWRKID	- Network Identifier
X..M..E	NINCODE	- Reporting Exception Code
X..M..E	SYSID	- System Identifier

X....E WEEK - Week of Year
X..M..E YEAR - Year of Century
X..M..E ZONE - Time Zone

Common Data Elements

X....E DAYNAME - Name of Day of Week
X..M.. DURATION - Recording Interval Time
X..M..E ENDTS - End Time Stamp
X..M.. MICSVER - CA MICS Version Number
X....E NCPNAME - Network Ctl Program Name
X....E NETNAME - Resource Network Name
X....E NPMIPADR - NPM IP Address
X..M.. NPMTMAOT - Actual Observation Time
X..M.. NPMTSEIS - Expected Interval Time
X..M.. NPMTSLOG - Time Record Logged To SMF
X..M..E PLUNETID - PLU Network Id
X..M..E PRODUCT - Network Product (Source) Name
X..M..E PRODVRL - Product Version and Release
X..M..E RESNAME - Resource Generic Name
X..M..E STARTTS - Start Time Stamp
X..M.. TMOFFSET - Time Offset

Retained Data Elements

X.... NINEVETS - Time Alert Was Recorded
X....E NINEXCRC - Exception/Resolution Reason Code
X..M.. NINMONNM - Alert Monitor Name
X..M.. NINNMEXA - Exception Generic Category
X..M.. NINNMEXT - Exception Type, Low Or High
X..M..E NINN RHIC - High Limit Criterion For Exception
X..M..E NINN RLOC - Low Limit Criterion For Exception
X....E NINN RTRI - Monitor Limit Triggered
X..M..E NINN RVAL - Value Of Monitored Element
X....E NINRESOL - Exception Resolution (Y/N)
X..M..E NINTYPE - Incident Type (E/R)
X....E NINUINID - Unique Incident ID
X..M.. NINUMSSG - User-specified Alert Description
X..M.. NINXDSKY - Cross Domain NetSpy Name

Accumulated Data Elements

X..M..E NINN RDER - Detached Resolution Count
X..M..E NINN REXI - Expired Intervals Since Exception
X..M.. NINN RHER - Total High Limit Value Difference
X..M.. NINN RHIR - High Limit Resolution Count
X..M.. NINN RHIX - High Limit Exception Count
X..M.. NINN RLER - Total Low Limit Value Difference
X..M.. NINN RLOR - Low Limit Resolution Count

X..M.. NINNRL0X - Low Limit Exception Count
X..M.. NINNRMRR - Number Of Monitor Resolutions
X..M.. NINNRMXR - Number Of Monitor Exceptions
X..M..E NINNSTR - Stopped Resolution Count

Derived Data Elements

X..M.. NINAVHER - Average High Limit Value Difference
X..M.. NINAVLER - Average Low Limit Value Difference

5.2.4.3 Usage Considerations

This section identifies the special considerations or techniques related to using the SNTNIN file, followed by several retrieval examples.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As the file's granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEK should not be used in MONTHS.
2. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7. For NPM, NETWRKID may be set to the value of PLU Network Identifier (PLUNETID).
 - o TMOFFSET - Time offset applied to the data in the file. The user can associate a time offset with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. Time offset is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

3. The following data elements lose significance once summarization has been performed. These data elements should only be referenced when the last observed value in a summarization interval is significant.

NPMTSLOG - Time Record Logged to SMF
NPMTSEIS - Expected Interval Time
RESNAME - Resource Generic Name
NINNRHIC - High Limit Criterion for the Exception
NINNRLOC - Low Limit Criterion for the Exception
NINNRVAL - Value of the Monitored Element

4. The following data elements are user-defined options specified in the NPM START MONITOR command and recorded in the SMF Type 38 record that is input to this file.

NINNRHIC - High Limit Criterion for the Exception
NINNRLOC - Low Limit Criterion for the Exception
NINNRVAL - Value of the Monitored Element

Retrieval Examples

1. Show the frequencies of each monitor exception by generic name, using month-to-date data:

```
PROC FREQ DATA=&PSNTM..SNTNIN00;  
  TABLES NINNMEXA * NINNRMXR / NOROW NOCOL; RUN;
```

2. Produce a chart of the number of monitor exception occurrences, by hour using yesterday's data:

```
PROC CHART DATA=&PSNTD..SNTNIN01;  
  VBAR HOUR / SUMVAR=NINNRMXR DISCRETE; RUN;
```

5.2.5 NPM User Activity File (SNTPSU)

The NPM User Activity File (SNTPSU) quantifies response time and network traffic statistics by user-defined account code for sessions between applications and terminals. The file is derived from NPM SMF records or the VM equivalent.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.5.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	YEAR	MONTH	DAY	
	HOUR	ENDTS				
DAYS	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	YEAR	MONTH	DAY	
	HOUR					
WEEKS	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	YEAR	WEEK	ZONE	
	HOUR					
MONTHS	N/A					
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=DISK option in effect. All computed data elements are kept on the file on auxiliary storage.

Figure 5-5. SNTPSU Timespan Granularity Chart

5.2.5.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

X - DETAIL
 D - DAYS
 W - WEEKS
 M - MONTHS
 Y - YEARS
 T - TABLES AREA
 . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XDW...E	HOURL	- Hour of Day
XD...E	MONTH	- Month of Year
XDW...E	NETWRKID	- Network Identifier
XDW...E	SNTACT1	- PRIMARY LOGICAL UNIT(PLU)
XDW...E	SNTACT2	- SLUSAPU NETV/NPM1.3,SLUSA NPM1.2 OR NSPY

XDW...E SNTACT3 - SLUPU IF NLDM OR NETSPY, SLU IF NPM
XDW...E SNTACT4 - NLDM PERFCLSS, NPM BLANK, NSPY/NAC SLU
XDW...E SNTACT5 - NOT-USED
XDW...E SYSID - System Identifier
XDW...E WEEK - Week of Year
XDW...E YEAR - Year of Century
XDW...E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
XDW... DURATION - Recording Interval Time
XDW...E ENDTS - End Time Stamp
XDW... INTERVLS - Number of Recording Intervals
XDW... MICSVER - CA MICS Version Number
X..... NETGROUP - Network Service Group
XDW...E NPMHIHST - High Threshold Time, For Host
XDW...E NPMHINET - High Threshold Time, For Network
XDW...E NPMHITOT - High Threshold Time, Total
X.....E NPMIPADR - NPM IP Address
XDW...E NPMLHST - Low Threshold Time, For Host
XDW...E NPMLONET - Low Threshold Time, For Network
XDW...E NPMLTOT - Low Threshold Time, Total
X.....E NPMPORT - NPM Port Number
XDW... NPMRVAL1 - Response Distribution Limits 1
XDW... NPMRVAL2 - Response Distribution Limits 2
XDW... NPMRVAL3 - Response Distribution Limits 3
XDW... NPMRVAL4 - Response Distribution Limits 4
XDW...E NPMVRR - NPM Version/Release Number
XDW...E ORGSYSID - Originating System Identification
XDW... PLU - Primary Logical Unit
XDW...E PLUNETID - PLU Network Id
XDW... PLUSA - Primary Logical Unit Subarea
XDW... PRODUCT - Network Product (Source) Name
XDW... SLU - Secondary Logical Unit
XD.... SLULINK - SLU Link
XDW...E SLUNETID - SLU Network Id
XD.... SLUPU - SLU Physical Unit
XDW... SLUSA - Secondary Logical Unit Subarea
XDW...E SNTAPU - PLU Subarea Physical Unit Name
XDW...E SNTSAPU - SLU Subarea Physical Unit Name
XDW...E STARTTS - Start Time Stamp
XDW... TMOFFSET - Time Offset

Retained Data Elements

X.....E PSUACCNT - Account Number
X.....E PSUGRPID - User Group ID
XD.... PSUHSA - Host Subarea Address

XD.... PSUIEXRT - Inbound Explicit Route Number
 X..... PSULDEV - Locally Attached Device (Y or N)
 XD.... PSUNODNM - Network Node Name
 XD.... PSUOEXRT - Outbound Explicit Route Number
 X.....E PSUSERID - User ID
 X.....E PSUSMID - Session Manager ID
 X.....E PSUSMPLU - Session Manager PLU
 X.....E PSUSMSLU - Session Manager SLU
 XD.... PSUSPUA - SLU PU Address
 XD.... PSUTRPTY - Transmission Priority
 XD.... PSUVRTE - Virtual Route Number

Accumulated Data Elements

XDW... PSUBDST1 - Response Dist Count 1 (Net and Host)
 XDW... PSUBDST2 - Response Dist Count 2 (Net and Host)
 XDW... PSUBDST3 - Response Dist Count 3 (Net and Host)
 XDW... PSUBDST4 - Response Dist Count 4 (Net and Host)
 XDW... PSUBDST5 - Response Dist Count 5 (Net and Host)
 XDW... PSUCOST - Billable Cost
 XDW... PSUERQTM - Total Time Exceeded Squared
 XDW... PSUERTTM - Total Time Oper Threshold Exceeded
 XDW... PSUHDST1 - Response Dist Count 1 (Host)
 XDW... PSUHDST2 - Response Dist Count 2 (Host)
 XDW... PSUHDST3 - Response Dist Count 3 (Host)
 XDW... PSUHDST4 - Response Dist Count 4 (Host)
 XDW... PSUHDST5 - Response Dist Count 5 (Host)
 XDW...E PSUHRESC - Resp Event Count (Host)
 XDW... PSUHRQTM - Host Resp Time Squared
 XDW... PSUHRSTM - Host Only Response Time
 XDW... PSUNNHTM - Network Resp Time
 XDW...E PSUNRESC - Resp Event Count (Net w/ Host Tx)
 XDW...E PSUNRFMR - No. of Text PIU Bytes Rec'd
 XDW...E PSUNRFMS - No. of Text PIU Bytes Sent
 XDW... PSUNRHO - No. of Host Only Transactions
 XDW...E PSUNRHRE - Resp Exceeded Count (Host)
 XDW... PSUNRMBR - No. of Text Message Bytes Rec'd
 XDW... PSUNRMBS - No. of Text Message Bytes Sent
 XDW... PSUNRMSR - No. of Text Messages Rec'd
 XDW... PSUNRMSS - No. of Text Messages Sent
 XDW...E PSUNRNFR - No. of Control PIU Bytes Rec'd
 XDW...E PSUNRNFS - No. of Control PIU Bytes Sent
 XDW... PSUNRNNH - Resp Event Count (Net)
 XDW...E PSUNRNRE - Resp Exceeded Count (Network)
 XDW...E PSUNRPFR - Number Text PIUs Received
 XDW...E PSUNRPFS - Number Text PIUs Sent
 XDW...E PSUNRPNR - Number Control PIUs Received
 XDW...E PSUNRPNS - Number Control PIUs Sent
 XDW... PSUNRQTM - Net Resp Time Squared (w/ Host Tx)

XDW... PSUNRSTM - Network Resp Time (w/ Host Tx)
XDW...E PSUNRTRE - Resp Exceeded Count (Total)
XDW... PSUORQTM - Network Resp Time Squared
XDW...E PSUTRESC - Resp Event Count (Total)
XDW... PSUTRQTM - Total Resp Time Squared
XDW... PSUTRSTM - Total Response Time

Maximum Data Elements

XDW... PSUMXHTM - Max Host Resp Time
XDW... PSUMXMBR - Max Text Message Received
XDW... PSUMXMBS - Max Text Message Sent
XDW... PSUMXNNH - Max Net Resp Time
XDW... PSUMXNTM - Max Net Resp Time (w/ Host Tx)
XDW... PSUMXTBR - Max Text PIU Rec'd
XDW... PSUMXTBS - Max Text PIU Sent
XDW... PSUMXTTM - Max Total Resp Time

Derived Data Elements

XDW... PSUAVFMR - Average Text PIU Rec'd
XDW... PSUAVFMS - Average Text PIU Sent
XDW... PSUAVHTM - Average Host Response Time
XDW... PSUAVNFR - Average Control PIU Rec'd
XDW... PSUAVNFS - Average Control PIU Sent
XDW... PSUAVNTM - Average Network Response Time
XDW... PSUAVTTM - Average Total Response Time
XDW... PSUBRESC - Resp Event Count (Both)
XDW...E PSUNRTCH - Total Bytes Transmitted
XDW... PSUPCBR1 - Cum. Pct Both Resp Within Limit 1
XDW... PSUPCBR2 - Cum. Pct Both Resp Within Limit 2
XDW... PSUPCBR3 - Cum. Pct Both Resp Within Limit 3
XDW... PSUPCBR4 - Cum. Pct Both Resp Within Limit 4
XDW... PSUPCHR1 - Cum. Pct Host Resp Within Limit 1
XDW... PSUPCHR2 - Cum. Pct Host Resp Within Limit 2
XDW... PSUPCHR3 - Cum. Pct Host Resp Within Limit 3
XDW... PSUPCHR4 - Cum. Pct Host Resp Within Limit 4
XDW... PSUPCNON - Pct of Total Events W/out Netwk Resp
XDW... PSUPCTR1 - Cum. Pct Total Resp Within Limit 1
XDW... PSUPCTR2 - Cum. Pct Total Resp Within Limit 2
XDW... PSUPCTR3 - Cum. Pct Total Resp Within Limit 3
XDW... PSUPCTR4 - Cum. Pct Total Resp Within Limit 4
XDW... PSUTDST1 - Response Dist Count 1 (Total)
XDW... PSUTDST2 - Response Dist Count 2 (Total)
XDW... PSUTDST3 - Response Dist Count 3 (Total)
XDW... PSUTDST4 - Response Dist Count 4 (Total)
XDW... PSUTDST5 - Response Dist Count 5 (Total)

5.2.5.3 Usage Considerations

This section identifies the special considerations or techniques related to using the SNTPSU file, followed by several retrieval examples.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As the file's granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEK should not be used in MONTHS.
2. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one- to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7. For NPM, NETWRKID may be set to the value of PLU Network Identifier (PLUNETID).
 - o TMOFFSET - Time offset applied to the data in the file. The user can associate a time offset with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. Time offset is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

3. The following data elements lose significance once summarization has been performed. These data elements should only be referenced when the last observed value in a summarization interval is significant.

NPMHIHST - High Threshold Time, For Host
NPMHINET - High Threshold Time, For Network
NPMHITOT - High Threshold Time, Total
NPMLOHST - Low Threshold Time, For Host
NPMLONET - Low Threshold Time, For Network
NPMLTOT - Low Threshold Time, Total
NPMRVAL1 - Response Distribution Limits 1
NPMRVAL2 - Response Distribution Limits 2
NPMRVAL3 - Response Distribution Limits 3
NPMRVAL4 - Response Distribution Limits 4
PLU - Primary Logical Unit
PLUSA - Primary Logical Unit Subarea
SLU - Secondary Logical Unit
SLULINK - SLU Link
SLUPU - SLU Physical Unit
SLUSA - Secondary Logical Unit Subarea
SLUNETID - SLU Network ID
TMOFFSET - Time Offset
PSUHSA - Host Subarea Address
PSUIEXRT - Inbound Explicit Route Number
PSUNODNM - Network Node Name
PSUOEXRT - Outbound Explicit Route Number
PSUSPUA - SLU PU Address
PSUTRPTY - Transmission Priority
PSUVR RTE - Virtual Route Number

4. Following is a brief discussion of NPM's techniques for measuring and recording various response time data.
 - o Host response - the amount of time required to turn the transaction around in the host. This time includes a small amount of VTAM time (NPM sits in the application subsystem interface) and all of the application (CICS, IMS, TS0) time.
 - o Network response - to measure and record network response time, NPM requires that either (1) each transaction request a definite response (DR) from the terminal, or (2) the NPM DYNAMIC DR feature- available only with NPM - be used to force the transaction into DR mode.
 - o Total response - the sum of host and network response

times.

There are, however, special considerations if this data is to be interpreted correctly. NPM maintains buckets to save the data in the three categories above. If definite response is neither requested nor forced for a particular transaction, there will be no network response time measure for that transaction. If all transactions during a session interval are in definite response mode (network response is measured), total response, as recorded by NPM, is complete.

However, when only some transactions within a session interval are in definite response mode, NPM computes the average network time (from the transactions that are in definite response mode) and adds this amount to the host time for each exception response mode transaction. The result is an estimated total response time. These estimates may or may not adequately reflect what the end user actually observed as total response time.

This file maintains a data element, PSUPCNON (Percent of Total Events Without Network Response) that is intended to convey some confidence factor for the usefulness of the total response data. For example, if 80% of the transactions within a session interval requested definite response, PSUPCNON will be 80%.

5. Unlike the other files in the SNT and NVS information areas, the SNTPSU may only be defined as ESSENTIAL ALL and DERIVED DISK. Any other values coded in the CPLXDEF member of sharedprefix.MICS.PARMS will be reset to these values during the SNTGEN process.

Retrieval Examples

1. Assume that the data center response time objectives state that 90% of all total responses must be less than five (5) seconds. Assuming NPM is parameterized such that NPMRVAL3 (response time limit bucket 3) is set at five (5) seconds, select those sessions not meeting the stated objective. List each session and relevant information.

```
DATA WKFILE;
  SET &PSNTX..SNTPSU01;
  IF PSUPCTR3 LT 90; /* SELECT LESS THAN 90 % */

PROC PRINT DATA=WKFILE;
  ID NETWRKID SYSID;
```

```
VAR PLU SLULINK SLU PSUAVHTM PSUAVNTM PSUAVTTM;
```

2. Chart total response time for Secondary Logical Unit (SLU-terminal) THC12 between 1 and 2 PM for the last five weeks. This example assumes that the choice for account code fields (SNTACT1-SNTACTn) resulted in data summarization to the terminal (SLU) level.

```
DATA COMBFILE;  
  SET &PSNTW..SNTPSU01 &PSNTW..SNTPSU02 &PSNTW..SNTPSU03  
    &PSNTW..SNTPSU04 &PSNTW..SNTPSU05 ;  
  IF SLU='THC12' AND HOUR=14;  
  
PROC CHART DATA=COMBFILE;  
  VBAR WEEK / SUMVAR=PSUAVTTM DISCRETE;
```

5.2.6 NPM System (PLU) Activity File (SNTPSY)

The NPM System (PLU) Activity File (SNTPSY) quantifies transaction response time and input and output character traffic by application (IMS, CICS, etc.). The file is derived from NPM SMF records or the VM equivalent.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.6.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	N/A					
DAYS	NETWRKID	SYSID	SNTPAPU	PLU	YEAR	
	MONTH	DAY	HOUR			
WEEKS	NETWRKID	SYSID	SNTPAPU	PLU	YEAR	
	WEEK	ZONE	HOUR			
MONTHS	NETWRKID	SYSID	SNTPAPU	PLU	YEAR	
	MONTH	ZONE				
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=DEfault option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-6. SNTPSY Timespan Granularity Chart

5.2.6.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

X - DETAIL
 D - DAYS
 W - WEEKS
 M - MONTHS
 Y - YEARS
 T - TABLES AREA
 . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

.D...E	DAY	- Day of Month
.DW...E	HOURL	- Hour of Day
.D.M..E	MONTH	- Month of Year
.DWM..E	NETWRKID	- Network Identifier
.DWM..E	PLU	- Primary Logical Unit
.DWM..E	SNTAPU	- PLU Subarea Physical Unit Name

.DWM..E SYSID - System Identifier
.DW...E WEEK - Week of Year
.DWM..E YEAR - Year of Century
.DWM..E ZONE - Time Zone

Common Data Elements

.D....E DAYNAME - Name of Day of Week
.DWM..E ENDTS - End Time Stamp
.DWM..E INTERVLS - Number of Recording Intervals
.DWM.. MICSVER - CA MICS Version Number
.DWM..E NPMHIHST - High Threshold Time, For Host
.DWM..E NPMHINET - High Threshold Time, For Network
.DWM..E NPMHITOT - High Threshold Time, Total
.DWM..E NPMLOHST - Low Threshold Time, For Host
.DWM..E NPMLONET - Low Threshold Time, For Network
.DWM..E NPMLTOT - Low Threshold Time, Total
.DWM..E NPMRVAL1 - Response Distribution Limits 1
.DWM..E NPMRVAL2 - Response Distribution Limits 2
.DWM..E NPMRVAL3 - Response Distribution Limits 3
.DWM..E NPMRVAL4 - Response Distribution Limits 4
.DWM..E NPMVRRL - NPM Version/Release Number
.DWM.. ORGSYSID - Originating System Identification
.DWM..E PLUNETID - PLU Network Id
.DWM..E PLUSA - Primary Logical Unit Subarea
.DWM.. PRODUCT - Network Product (Source) Name
..... SLU - Secondary Logical Unit
..... SLULINK - SLU Link
..... SLUPU - SLU Physical Unit
.DWM.. SLUSA - Secondary Logical Unit Subarea
.DWM..E SNTSAPU - SLU Subarea Physical Unit Name
.DWM..E STARTTS - Start Time Stamp
.DWM.. TMOFFSET - Time Offset

Retained Data Elements

.D.... PSYHSA - Host Subarea Address
.D.... PSYIEXRT - Inbound Explicit Route Number
.D.... PSYNODNM - Network Node Name
.D.... PSYOEEXRT - Outbound Explicit Route Number
.D.... PSYSPUA - SLU PU Address
.D.... PSYTRPTY - Transmission Priority
.D.... PSYVRTE - Virtual Route Number

Accumulated Data Elements

.DWM..E PSYBDST1 - Response Dist Count 1 (Net and Host)
.DWM..E PSYBDST2 - Response Dist Count 2 (Net and Host)
.DWM..E PSYBDST3 - Response Dist Count 3 (Net and Host)

.DWM..E PSYBDST4 - Response Dist Count 4 (Net and Host)
 .DWM.. PSYBDST5 - Response Dist Count 5 (Net and Host)
 .DWM.. PSYERQTM - Total Time Exceeded Squared
 .DWM.. PSYERTTM - Total Time Oper Threshold Exceeded
 .DWM..E PSYHDST1 - Response Dist Count 1 (Host)
 .DWM..E PSYHDST2 - Response Dist Count 2 (Host)
 .DWM..E PSYHDST3 - Response Dist Count 3 (Host)
 .DWM..E PSYHDST4 - Response Dist Count 4 (Host)
 .DWM.. PSYHDST5 - Response Dist Count 5 (Host)
 .DWM..E PSYHRESC - Resp Event Count (Host)
 .DWM.. PSYHRQTM - Host Response Time Squared
 .DWM..E PSYHRSTM - Host Only Response Time
 .DWM.. PSYNNHTM - Network Resp Time
 .DWM..E PSYNRESC - Resp Event Count (Net w/ Host Tx)
 .DW...E PSYNRFMR - No. Of Text PIU Bytes Rec'd
 .DW...E PSYNRFMS - No. Of Text PIU Bytes Sent
 .DWM.. PSYNRHO - No. of Host Only Transactions
 .DWM..E PSYNRHRE - Resp Exceeded Count (Host)
 .DWM.. PSYNRMBR - No. of Text Message Bytes Rec'd
 .DWM.. PSYNRMBS - No. of Text Message Bytes Sent
 .DWM.. PSYNRMSR - No. of Text Messages Rec'd
 .DWM.. PSYNRMSS - No. of Text Messages Sent
 .DW...E PSYNRNFR - No. Of Control PIU Bytes Rec'd
 .DW...E PSYNRNFS - No. Of Control PIU Bytes Sent
 .DWM.. PSYNRNNH - Resp Event Count (Net)
 .DWM..E PSYNRNRE - Resp Exceeded Count (Network)
 .DW...E PSYNRPFR - Number Text PIUs Received
 .DW...E PSYNRPFS - Number Text PIUs Sent
 .DW...E PSYNRPNR - Number Control PIUs Received
 .DW...E PSYNRPNS - Number Control PIUs Sent
 .DWM.. PSYNRQTM - Net Resp Time Squared (w/ Host Tx)
 .DWM..E PSYNRSTM - Network Resp Time (w/ Host Tx)
 .DWM..E PSYNRTRE - Resp Exceeded Count (Total)
 .DWM.. PSYORQTM - Network Resp Time Squared
 .DWM..E PSYTRESC - Resp Event Count (Total)
 .DWM.. PSYTRQTM - Total Resp Time Squared
 .DWM..E PSYTRSTM - Total Response Time

Maximum Data Elements

.DWM.. PSYMXHTM - Max Host Resp Time
 .DWM.. PSYMXMBR - Max Text Message Received
 .DWM.. PSYMXMBS - Max Text Message Sent
 .DWM.. PSYMXNNH - Max Net Resp Time
 .DWM.. PSYMXNTM - Max Net Resp Time (w/ Host Tx)
 .DWM.. PSYMXTBR - Max Text PIU Received
 .DWM.. PSYMXTBS - Max Text PIU Sent
 .DWM..E PSYMXTTM - Max Total Resp Time

Derived Data Elements

.DW...E PSYAVFMR - Average Text PIU Rec'd
.DW...E PSYAVFMS - Average Text PIU Sent
.DWM..E PSYAVHTM - Average Host Response Time
.DW...E PSYAVNFR - Average Control PIU Rec'd
.DW...E PSYAVNFS - Average Control PIU Sent
.DWM..E PSYAVNTM - Average Network Response Time
.DWM..E PSYAVTTM - Average Total Response Time
.DWM.. PSYBRES - Resp Event Count (Both)
.DWM.. PSYPCBR1 - Cum. Pct Both Resp Within Limit 1
.DWM.. PSYPCBR2 - Cum. Pct Both Resp Within Limit 2
.DWM.. PSYPCBR3 - Cum. Pct Both Resp Within Limit 3
.DWM.. PSYPCBR4 - Cum. Pct Both Resp Within Limit 4
.DWM.. PSYPCHR1 - Cum. Pct Host Resp Within Limit 1
.DWM.. PSYPCHR2 - Cum. Pct Host Resp Within Limit 2
.DWM.. PSYPCHR3 - Cum. Pct Host Resp Within Limit 3
.DWM.. PSYPCHR4 - Cum. Pct Host Resp Within Limit 4
.DWM.. PSYPCNON - Pct of Total Events W/out Netwk Resp
.DWM..E PSYPCTR1 - Cum. Pct Total Resp Within Limit 1
.DWM..E PSYPCTR2 - Cum. Pct Total Resp Within Limit 2
.DWM..E PSYPCTR3 - Cum. Pct Total Resp Within Limit 3
.DWM..E PSYPCTR4 - Cum. Pct Total Resp Within Limit 4
.DWM..E PSYTDST1 - Cum. Response Dist Count 1 (Total)
.DWM..E PSYTDST2 - Cum. Response Dist Count 2 (Total)
.DWM..E PSYTDST3 - Cum. Response Dist Count 3 (Total)
.DWM..E PSYTDST4 - Cum. Response Dist Count 4 (Total)
.DWM.. PSYTDST5 - Cum. Response Dist Count 5 (Total)

5.2.6.3 Usage Considerations

This section identifies the special considerations or techniques related to using the SNTPSY file, followed by several retrieval examples.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As the file's granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEK should not be used in MONTHS.
2. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7. For NPM, NETWRKID may be set to the value of PLU Network Identifier (PLUNETID).
 - o TMOFFSET - Time offset applied to the data in the file. The user can associate a time offset with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. Time offset is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

3. The following data elements lose significance once summarization has been performed. These data elements should be referenced only when the last observed value in a summarization interval is significant.

NPMHIHST - High Threshold Time, For Host
NPMHINET - High Threshold Time, For Network
NPMHITOT - High Threshold Time, Total
NPMLOHST - Low Threshold Time, For Host
NPMLONET - Low Threshold Time, For Network
NPMLTOT - Low Threshold Time, Total
NPMRVAL1 - Response Distribution Limits 1
NPMRVAL2 - Response Distribution Limits 2
NPMRVAL3 - Response Distribution Limits 3
NPMRVAL4 - Response Distribution Limits 4
SLU - Secondary Logical Unit
SLULINK - SLU Link
SLUPU - SLU Physical Unit
SLUSA - Secondary Logical Unit Subarea
TMOFFSET - Time Offset
PSYHSA - Host Subarea Address
PSYIEXRT - Inbound Explicit Route Number
PSYNODNM - Network Node Name
PSY0EXRT - Outbound Explicit Route Number
PSYSPUA - SLU PU Address
PSYTRPTY - Transmission Priority
PSYVRTE - Virtual Route Number

4. Following is a brief discussion of NPM's techniques for measuring and recording various response time data.
- o Host response - the amount of time required to turn the transaction around in the host. This time includes a small amount of VTAM time (NPM sits in the application subsystem interface) and all of the application (CICS, IMS, TS0) time.
 - o Network response - to measure and record network response time, NPM requires that either (1) each transaction request a definite response (DR) from the terminal, or (2) the NPM DYNAMIC DR feature (available only with NPM) be used to force the transaction into DR mode.
 - o Total response - the sum of host and network response times.

There are, however, special considerations if this data is

to be interpreted correctly. NPM maintains buckets to save the data in the three categories above. If definite response is neither requested nor forced for a particular transaction, there will be no network response time measure for that transaction. If all transactions during a session interval are in definite response mode (network response is measured), total response, as recorded by NPM, is complete.

However, when only some transactions within a session interval are in definite response mode, NPM computes the average network time (from the transactions that are in definite response mode) and adds this amount to the host time for each exception response mode transaction. The result is an estimated total response time. These estimates may or may not adequately reflect what the end user actually observed as total response time.

This file maintains a data element, PSYPCNON (Percent of Total Events Without Network Response) that is intended to convey some confidence factor for the usefulness of the total response data. For example, if 80% of the transactions within a session interval requested definite response, PSUPCNON will be 80%.

Retrieval Example

Chart response time for Primary Logical Unit (PLU) PRODCICS. Break the chart bars into host and network response time. Use yesterday's data.

```
%LET BY = PLU HOUR ;
%LET BREAK = HOUR ;

PROC SORT DATA=&PSNTD..SNTPSY01 OUT=WKPSY;
  BY &BY;

DATA WKPSY;
  SET WKPSY;
  %PSYSUM
RUN;

DATA WKPSY;
  SET WKPSY;
  IF PLU='PRODCICS';
  RESPONSE=PSYAVNTM; TYPERESP='NETWORK'; OUTPUT;
  RESPONSE=PSYAVHTM; TYPERESP='HOST  '; OUTPUT;

PROC CHART DATA=WKPSY;
```

```
VBAR HOUR / SUMVAR=RESPONSE  
SUBGROUP=TYPESP  
DISCRETE;RUN;
```

5.2.7 NPM Link Activity File (SNTNPL)

The NPM Link Activity File (SNTNPL) quantifies transaction response time and input and output character traffic by physical unit so that total activity for each network link (line) can be determined. The file is derived from NPM SMF records or the VM equivalent.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.7.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	N/A					
DAYS	NETWRKID	SYSID	SNTSAPU	SLULINK	SLUPU	
	SNTPAPU	PLU	YEAR	MONTH	DAY	
	HOUR					
WEEKS	NETWRKID	SYSID	SNTSAPU	SLULINK	SLUPU	
	SNTPAPU	PLU	YEAR	WEEK	ZONE	
	HOUR					
MONTHS	NETWRKID	SYSID	SNTSAPU	SLULINK	SLUPU	
	SNTPAPU	PLU	YEAR	MONTH	ZONE	
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-7. SNTNPL Timespan Granularity Chart

5.2.7.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

X - DETAIL
 D - DAYS
 W - WEEKS
 M - MONTHS
 Y - YEARS
 T - TABLES AREA
 . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

.D...E	DAY	- Day of Month
.DW...E	HOURL	- Hour of Day
.D.M..E	MONTH	- Month of Year
.DWM..E	NETWRKID	- Network Identifier
.DWM..E	PLU	- Primary Logical Unit
.DWM..E	SLULINK	- SLU Link

.DWM..E SLUPU - SLU Physical Unit
.DWM..E SNTPAU - PLU Subarea Physical Unit Name
.DWM..E SNTSAU - SLU Subarea Physical Unit Name
.DWM..E SYSID - System Identifier
.DW...E WEEK - Week of Year
.DWM..E YEAR - Year of Century
.DWM..E ZONE - Time Zone

Common Data Elements

.D....E DAYNAME - Name of Day of Week
.DWM..E ENDTS - End Time Stamp
.DWM..E INTERVLS - Number of Recording Intervals
.DWM.. LNKTPCID - Network Link TP Circuit Id
.DWM.. MICSVER - CA MICS Version Number
.DWM..E NPMHIHST - High Threshold Time, For Host
.DWM..E NPMHINET - High Threshold Time, For Network
.DWM..E NPMHITOT - High Threshold Time, Total
.DWM..E NPMLOHST - Low Threshold Time, For Host
.DWM..E NPMLONET - Low Threshold Time, For Network
.DWM..E NPMLTOT - Low Threshold Time, Total
.DWM..E NPMRVAL1 - Response Distribution Limits 1
.DWM..E NPMRVAL2 - Response Distribution Limits 2
.DWM..E NPMRVAL3 - Response Distribution Limits 3
.DWM..E NPMRVAL4 - Response Distribution Limits 4
.DWM..E NPMVRRL - NPM Version/Release Number
.DWM..E PLUNETID - PLU Network Id
.DWM..E PLUSA - Primary Logical Unit Subarea
.DWM.. PRODUCT - Network Product (Source) Name
.DWM..E SLUSA - Secondary Logical Unit Subarea
.DWM..E STARTTS - Start Time Stamp
.DWM.. TMOFFSET - Time Offset

Retained Data Elements

.D.... NPLHSA - Host Subarea Address
.D.... NPLIEXRT - Inbound Explicit Route Number
.D.... NPLNODNM - Network Node Name
.D.... NPLQEXRT - Outbound Explicit Route Number
.D.... NPLSPUA - SLU PU Address
.D.... NPLTRPTY - Transmission Priority
.D.... NPLVRTE - Virtual Route Number

Accumulated Data Elements

.DWM..E NPLBDST1 - Response Dist Count 1 (Net and Host)
.DWM..E NPLBDST2 - Response Dist Count 2 (Net and Host)
.DWM..E NPLBDST3 - Response Dist Count 3 (Net and Host)
.DWM..E NPLBDST4 - Response Dist Count 4 (Net and Host)

.DWM.. NPLBDST5 - Response Dist Count 5 (Net and Host)
 .DWM.. NPLERQTM - Total Time Exceeded Squared
 .DWM.. NPLERTTM - Total Time Oper Threshold Exceeded
 .DWM..E NPLHDST1 - Response Dist Count 1 (Host)
 .DWM..E NPLHDST2 - Response Dist Count 2 (Host)
 .DWM..E NPLHDST3 - Response Dist Count 3 (Host)
 .DWM..E NPLHDST4 - Response Dist Count 4 (Host)
 .DWM.. NPLHDST5 - Response Dist Count 5 (Host)
 .DWM..E NPLHRESC - Resp Event Count (Host)
 .DWM.. NPLHRQTM - Host Response Time Squared
 .DWM..E NPLHRSTM - Host Only Response Time
 .DWM.. NPLNNHTM - Network Resp Time
 .DWM..E NPLNRESC - Resp Event Count (Net w/ Host Tx)
 .DWM.. NPLNRFMR - No. Of Text PIU Bytes Rec'd
 .DWM.. NPLNRFMS - No. Of Text PIU Bytes Sent
 .DWM.. NPLNRHO - No. of Host Only Transactions
 .DWM..E NPLNRHRE - Resp Exceeded Count (Host)
 .DWM.. NPLNRMBS - No. of Text Message Bytes Rec'd
 .DWM.. NPLNRMBR - No. of Text Message Bytes Sent
 .DWM.. NPLNRMSR - No. of Text Messages Rec'd
 .DWM.. NPLNRMSS - No. of Text Messages Sent
 .DWM.. NPLNRNFR - No. Of Control PIU Bytes Rec'd
 .DWM.. NPLNRNFS - No. Of Control PIU Bytes Sent
 .DWM.. NPLNRNNH - Resp Event Count (Net)
 .DWM..E NPLNRNRE - Resp Exceeded Count (Network)
 .DWM.. NPLNRPFR - Number Text PIUs Received
 .DWM.. NPLNRPFS - Number Text PIUs Sent
 .DWM.. NPLNRPNR - Number Control PIUs Received
 .DWM.. NPLNRPNS - Number Control PIUs Sent
 .DWM.. NPLNRQTM - Net Resp Time Squared (w/ Host Tx)
 .DWM..E NPLNRSTM - Network Resp Time (w/ Host Tx)
 .DWM..E NPLNRTRE - Resp Exceeded Count (Total)
 .DWM.. NPLORQTM - Network Resp Time Squared
 .DWM..E NPLTRES - Resp Event Count (Total)
 .DWM.. NPLTRQTM - Total Resp Time Squared
 .DWM..E NPLTRSTM - Total Response Time

Maximum Data Elements

.DWM..E NPLMXHTM - Max Host Resp Time
 .DWM.. NPLMXMBR - Max Text Message Received
 .DWM.. NPLMXMBS - Max Text Message Sent
 .DWM.. NPLMXNNH - Max Net Resp Time
 .DWM..E NPLMXNTM - Max Net Resp Time (w/ Host Tx)
 .DWM.. NPLMXTBR - Max Text PIU Received
 .DWM.. NPLMXTBS - Max Text PIU Sent
 .DWM..E NPLMXTTM - Max Total Resp Time

Derived Data Elements

.DW... NPLAVFMR - Average Text PIU Rec'd
.DW... NPLAVFMS - Average Text PIU Sent
.DWM..E NPLAVHTM - Average Host Response Time
.DW... NPLAVNFR - Average Control PIU Rec'd
.DW... NPLAVNFS - Average Control PIU Sent
.DWM..E NPLAVNTM - Average Network Response Time
.DWM..E NPLAVTTM - Average Total Response Time
.DWM.. NPLBRES - Resp Event Count (Both)
.DWM.. NPLPCBR1 - Cum. Pct Both Resp Within Limit 1
.DWM.. NPLPCBR2 - Cum. Pct Both Resp Within Limit 2
.DWM.. NPLPCBR3 - Cum. Pct Both Resp Within Limit 3
.DWM.. NPLPCBR4 - Cum. Pct Both Resp Within Limit 4
.DWM.. NPLPCHR1 - Cum. Pct Host Resp Within Limit 1
.DWM.. NPLPCHR2 - Cum. Pct Host Resp Within Limit 2
.DWM.. NPLPCHR3 - Cum. Pct Host Resp Within Limit 3
.DWM.. NPLPCHR4 - Cum. Pct Host Resp Within Limit 4
.DWM.. NPLPCLBS - NPM Percent Link Busy
.DWM.. NPLPCNON - Pct of Total Events W/out Netwk Resp
.DWM..E NPLPCTR1 - Cum. Pct Total Resp Within Limit 1
.DWM..E NPLPCTR2 - Cum. Pct Total Resp Within Limit 2
.DWM..E NPLPCTR3 - Cum. Pct Total Resp Within Limit 3
.DWM..E NPLPCTR4 - Cum. Pct Total Resp Within Limit 4
.DWM..E NPLTDST1 - Response Dist Count 1 (Total)
.DWM..E NPLTDST2 - Response Dist Count 2 (Total)
.DWM..E NPLTDST3 - Response Dist Count 3 (Total)
.DWM..E NPLTDST4 - Response Dist Count 4 (Total)
.DWM.. NPLTDST5 - Response Dist Count 5 (Total)

5.2.7.3 Usage Considerations

This section identifies the special considerations or techniques related to using the SNTNPL file, followed by several retrieval examples.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As the file's granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEK should not be used in MONTHS.
2. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7. For NPM, NETWRKID may be set to the value of PLU Network Identifier (PLUNETID).
 - o LNKTPCID - Link TP Circuit ID value. This data element will typically contain the value of the link vendor's (AT&T, MCI, etc.) billing identifier. It is set in the Link TP Circuit Id Exit Routine, SNTCIDRT, discussed in Chapter 7.
 - o TMOFFSET - Time offset applied to the data in the file. The user can associate a time offset with each unique NETWRKID/SYSID combination. This offset is used to

adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. Time offset is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

3. The following data elements lose significance once summarization has been performed. These data elements should only be referenced when the last observed value in a summarization interval is significant.

LNKTPCID - Link TP Circuit Id
NPMHIHST - High Threshold Time, For Host
NPMHINET - High Threshold Time, For Network
NPMHITOT - High Threshold Time, Total
NPMLOHST - Low Threshold Time, For Host
NPMLONET - Low Threshold Time, For Network
NPMLOTOT - Low Threshold Time, Total
NPMRVAL1 - Response Distribution Limits 1
NPMRVAL2 - Response Distribution Limits 2
NPMRVAL3 - Response Distribution Limits 3
NPMRVAL4 - Response Distribution Limits 4
TMOFFSET - Time Offset
NPLHSA - Host Subarea Address
NPLIEXRT - Inbound Explicit Route Number
NPLNODNM - Network Node Name
NPLOEXRT - Outbound Explicit Route Number
NPLSPUA - SLU PU Address
NPLTRPTY - Transmission Priority
NPLVR RTE - Virtual Route Number

4. Following is a brief discussion of NPM's techniques for measuring and recording various response time data.
 - o Host response - the amount of time required to turn the transaction around in the host. This time includes a small amount of VTAM time (NPM sits in the application subsystem interface) and all of the application (CICS, IMS, TS0) time.
 - o Network response - to measure and record network response time, NPM requires that either (1) each transaction request a definite response (DR) from the terminal, or (2) the NPM DYNAMIC DR feature (available only with NPM) be used to force the transaction into DR mode.
 - o Total response - the sum of host and network response

times.

There are, however, special considerations if this data is to be interpreted correctly. NPM maintains buckets to save the data in the three categories above. If definite response is neither requested nor forced for a particular transaction, there will be no network response time measure for that transaction. If all transactions during a session interval are in definite response mode (network response is measured), total response, as recorded by NPM, is complete.

However, when only some transactions within a session interval are in definite response mode, NPM computes the average network time (from the transactions that are in definite response mode) and adds this amount to the host time for each exception response mode transaction. The result is an estimated total response time. These estimates may or may not adequately reflect what the end user actually observed as total response time.

This file maintains a data element, NPLPCNON (Percent of Total Events Without Network Response) that is intended to convey some confidence factor for the usefulness of the total response data. For example, if 80% of the transactions within a session interval requested definite response, PSUPCNON will be 80%.

Retrieval Examples

1. Chart response time for link (line) LHC1. Break the chart bars down into host and network response time. Use yesterday's data.

```
%LET BY = SLULINK HOUR ;
%LET BREAK = HOUR ;

PROC SORT DATA=&PSNTD..SNTNPL01 OUT=WKNPL;
  BY &BY;

DATA WKNPL;
  SET WKNPL;
  %NPLSUM
RUN;

DATA WKNPL;
  SET WKNPL;
  IF SLULINK='LHC1';
  RESPONSE=NPLAVNTM; TYPERESP='NETWORK'; OUTPUT;
```

```
RESPONSE=NPLAVHTM; TYPERESP='HOST  '; OUTPUT;
```

```
PROC CHART DATA=WKNPL;  
  VBAR HOUR / SUMVAR=RESPONSE  
    SUBGROUP=TYPERESP  
  DISCRETE;RUN;
```

2. Calculate percent link busy by hour for a group of links.
Link speed is provided by user code (below). Use month-to-date data.

```
%LET BY = SLULINK HOUR ;  
%LET BREAK = HOUR ;  
  
PROC SORT DATA=&PSNTM..SNTNPL00 OUT=WKNPL;  
  BY &BY;  
  
DATA WKNPL;  
  SET WKNPL;  
  %NPLSUM  
RUN;  
  
DATA WKNPL;  
  SET WKNPL;  
  IF SLULINK=:'LH';  
  IF SLULINK='LHC1' THEN LINKSPD=4800;  
  ELSE IF SLULINK='LHC2' THEN LINKSPD=9600;  
  ELSE IF SLULINK='LHC9' THEN LINKSPD=19600;  
  ELSE DELETE;  
  DURATION = ENDTS - STARTTS;  
  NPLPCLBS=((NPLNRNFR+NPLNRNFS+NPLNRFMR+NPLNRFMS) /  
    ((LINKSPD / 8) * DURATION)) * 100;  
  FORMAT NPLPCLBS MAPCT.;  
  
PROC CHART DATA=WKNPL;  
  BY SLULINK;  
  VBAR HOUR / SUMVAR=NPLPCLBS  
    DISCRETE;RUN;
```

5.2.8 NPDA Event File (SNTNEF)

The NPDA Event File (SNTNEF) quantifies, by event type and general and specific cause, conditions recorded by NetView and CA NetMaster as events both within the network and for channel-attached network communication devices. The file is derived from the NetView Hardware Monitor External Log record, the NPDA Report record, or the CA NetMaster NEWS SMF record.

Events for LAN resources are excluded from this file. They are written to the NPDA LAN File (SNTLNF), which contains all NPDA reliability data for LAN resources.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.8.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	NEFTEVNT	NEFFRTYP	NEFFRNAM	
	NEFGEVCC	NEFSEVCC	YEAR	MONTH	DAY	
	HOUR	ENDTS				
DAYS	NETWRKID	SYSID	NEFTEVNT	NEFFRTYP	NEFFRNAM	
	NEFGEVCC	NEFSEVCC	YEAR	MONTH	DAY	
	HOUR					
WEEKS	NETWRKID	SYSID	NEFTEVNT	NEFFRTYP	NEFFRNAM	
	NEFGEVCC	NEFSEVCC	YEAR	WEEK	ZONE	
	HOUR					
MONTHS	NETWRKID	SYSID	NEFTEVNT	NEFFRTYP	NEFFRNAM	
	NEFGEVCC	NEFSEVCC	YEAR	MONTH	ZONE	
YEARS	NETWRKID	SYSID	NEFTEVNT	NEFFRTYP	NEFFRNAM	
	NEFGEVCC	NEFSEVCC	YEAR	ZONE		
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=DEFAULT option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-8. SNTNEF Timespan Granularity Chart

5.2.8.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XDW...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWMY.E	NEFFRNAME	- Failing Resource Name
XDWMY.E	NEFFRTYP	- Failing Resource Type
XDWMY.E	NEFGEVCC	- General Event Cause Code

XDWMY.E NEFSEVCC - Specific Event Cause Code
XDWMY.E NEFTEVNT - Type of Event
XDWMY.E NETWRKID - Network Identifier
XDWMY.E SYSID - System Identifier
XDW...E WEEK - Week of Year
XDWMY.E YEAR - Year of Century
XDWMY.E ZONE - Time Zone

Common Data Elements

XD...E DAYNAME - Name of Day of Week
XDWMY.E ENDTS - End Time Stamp
XDWMY. MICSVER - CA MICS Version Number
XDWMY. PRODUCT - Network Product (Source) Name
XDWMY. PRODVRL - Product Version and Release
XDWMY.E STARTTS - Start Time Stamp
XDWMY. TMOFFSET - Time Offset

Retained Data Elements

XDWMY.E NEFACTCD - Event Action Code
XDWMY.E NEFBLKCD - Event Block Code
XDWMY. NEFCPLI - Complex Link Indicator (Y or N)
XDWMY. NEFDMNAM - Domain Name
XDWMY. NEFDQFR1 - Detail Qualifier 1
XDWMY. NEFDQFR2 - Detail Qualifier 2
XDWMY. NEFDQFR3 - Detail Qualifier 3
XDWMY.E NEFERRDS - Error Description: Probable Cause
X..... NEFEVETS - Event Time Stamp
XDWMY. NEFEVRTY - Event Resource Type
XDWMY. NEFFRNM1 - Resource Level Name 1
XDWMY. NEFFRNM2 - Resource Level Name 2
XDWMY. NEFFRNM3 - Resource Level Name 3
XDWMY. NEFFRNM4 - Resource Level Name 4
XDWMY. NEFFRNM5 - Resource Level Name 5
XDWMY. NEFFRTY1 - Resource Level Type 1
XDWMY. NEFFRTY2 - Resource Level Type 2
XDWMY. NEFFRTY3 - Resource Level Type 3
XDWMY. NEFFRTY4 - Resource Level Type 4
XDWMY. NEFFRTY5 - Resource Level Type 5

Accumulated Data Elements

XDWMY.E NEFNRLT - Number of Alerts
XDWMY.E NEFNREVT - Number of Events

5.2.8.3 Usage Considerations

This section identifies the special considerations or techniques related to using the SNTNEF File. Additionally, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As the files granularity increases in higher timespans certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEK should not be used in MONTHS.
2. The following data elements are user-defined. The value in each is dependent on user-selected options or user supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - Time offset applied to the data in the file. The user can associate a time offset with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. Time offset is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.
3. The following data elements lose significance once

summarization has been performed. These data elements should only be referenced when the last observed value in a summarization interval is significant.

NPDAVRRL - NPDA Version/Release
TMOFFSET - Time Offset
NEFCMPII - Complex Link Indicator (Y or N)

Retrieval Examples

1. Produce a count of the number of NPDA Events by resource type. Use last week's data.

```
PROC FREQ DATA=&PSNTW..SNTNEF01;  
  TABLES NEFFRTYP / NOROW NOCUM NOCOL;  
  WEIGHT NEFNREVT;
```

2. Produce a report showing the 50 resources having the highest incident rate for NPDA Event Alerts. Use last month's data.

```
PROC SORT DATA=&PSNTM..SNTNEF01 OUT=WKNEF;  
  BY DESCENDING NEFNRLT;
```

```
OPTIONS OBS=50;
```

```
PROC PRINT DATA=WKNEF;  
  ID NEFFRTYP NEFFRNM;  
  VAR NEFNREVT NEFNRLT NEFERRDS;
```

5.2.9 NPDA Statistical File (SNTNSF)

The NPDA Statistical File (SNTNSF) quantifies, by failing resource name and type, the total network traffic and number of temporary errors for network resources and channel-attached resources.

The file is derived from the NetView Hardware Monitor External Log record, the NPDA Report record, or the CA NetMaster NEWS SMF record.

Statistics for LAN resources are excluded from this file. They are written to the NPDA LAN File (SNTLNF), which contains all NPDA data for LAN resources.

NPDA statistics that accompany generic events (events that are logged to SMF at the same time as generic events) and that are for non-LAN resources are excluded from the NPDA Statistical file. These statistics are written to the NPDA Generic Alert File (SNTGAF).

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.9.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	NSFFRTYP	NSFFRNAM	YEAR	
	MONTH	DAY	HOUR	ENDTS		
DAYS	NETWRKID	SYSID	NSFFRTYP	NSFFRNAM	YEAR	
	MONTH	DAY	HOUR			
WEEKS	NETWRKID	SYSID	NSFFRTYP	NSFFRNAM	YEAR	
	WEEK	ZONE	HOUR			
MONTHS	NETWRKID	SYSID	NSFFRTYP	NSFFRNAM	YEAR	
	MONTH	ZONE				
YEARS	NETWRKID	SYSID	NSFFRTYP	NSFFRNAM	YEAR	
	ZONE					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=DEFAult option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-9. SNTNSF Timespan Granularity Chart

5.2.9.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD....E	DAY	- Day of Month
XDW...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWMY.E	NETWKID	- Network Identifier
XDWMY.E	NSFFRNAM	- Failing Resource Name
XDWMY.E	NSFFRTYP	- Failing Resource Type
XDWMY.E	SYSID	- System Identifier
XDW...E	WEEK	- Week of Year
XDWMY.E	YEAR	- Year of Century
XDWMY.E	ZONE	- Time Zone

Common Data Elements

XD....E	DAYNAME	- Name of Day of Week
XDWMY.E	ENDTS	- End Time Stamp
XDWMY.	MICSVER	- CA MICS Version Number
XDWMY.	PRODUCT	- Network Product (Source) Name
XDWMY.	PRODVRL	- Product Version and Release
XDWMY.E	STARTTS	- Start Time Stamp
XDWMY.	TMOFFSET	- Time Offset

Retained Data Elements

XDW...	NSFCPLI	- Complex Link Indicator (Y or N)
XDW...	NSFDMNAM	- Domain Name
X.....	NSFEVETS	- Event Time Stamp
XDW...	NSFFRNM1	- Resource Level Name 1
XDW...	NSFFRNM2	- Resource Level Name 2
XDW...	NSFFRNM3	- Resource Level Name 3
XDW...	NSFFRNM4	- Resource Level Name 4
XDW...	NSFFRNM5	- Resource Level Name 5
XDW...	NSFFRTY1	- Resource Level Type 1
XDW...	NSFFRTY2	- Resource Level Type 2
XDW...	NSFFRTY3	- Resource Level Type 3
XDW...	NSFFRTY4	- Resource Level Type 4
XDW...	NSFFRTY5	- Resource Level Type 5

Accumulated Data Elements

XDWMY.E NSFNRALT - Number of Alerts
XDWMY.E NSFNRSEA - Count of Stat with Event and Alert
XDWMY.E NSFTTERR - Total Temporary Errors
XDWMY.E NSFTTRFC - Total Traffic

Derived Data Elements

XDWMY.E NSFPCERR - Pct of Total Traffic w/ Temp Errors

5.2.9.3 Usage Considerations

This section identifies the special considerations or techniques related to using the SNTNSF File. Additionally, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As the files' granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEK should not be used in MONTHS.
2. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - Time offset applied to the data in the file. The user can associate a time offset with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. Time offset is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

3. The following data elements lose significance once summarization has been performed. These data elements should only be referenced when the last observed value in a summarization interval is significant.

NPDAVRRL - NPDA Version/Release
TMOFFSET - Time Offset
NSFCPLI - Complex Link Indicator (Y or N)

Retrieval Examples

1. Produce a count of the number of alerts by resource type. Use last week's data.

```
PROC FREQ DATA=&PSNTW..SNTNSF01;  
  TABLES NSFFRTYP / NOROW NOCUM NOCOL;  
  WEIGHT NSFNRLT;
```

2. Produce a report showing those resources having the highest ratio of temporary errors to total traffic. Use last month's data.

```
DATA WKNSF;  
  SET &PSNTM..SNTNSF01;  
  IF NSFPCERR GT 50;  
  
PROC PRINT DATA=WKNSF;  
  ID NSFFRTYP NSFFRNM;  
  VAR NSFTTRFC NSFTTERR;
```

5.2.10 NPDA LAN File (SNTLNF)

The NPDA LAN File (SNTLNF) quantifies, by failing resource name and type, the total number of alerts (both generic and standard), events, and statistics recorded by the NetView Hardware Monitor for LAN resources. The file is derived from the NetView Hardware Monitor External Log record.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.10.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	SNTTEVNT	SNTFRTYP	SNTFRNAM	
	SNTGEVCC	SNTSEVCC	SNTGPID	SNTGAID	YEAR	
	MONTH	DAY	HOUR	ENDTS		
DAYS	NETWRKID	SYSID	SNTTEVNT	SNTFRTYP	SNTFRNAM	
	SNTGEVCC	SNTSEVCC	SNTGPID	SNTGAID	YEAR	
	MONTH	DAY	HOUR			
WEEKS	NETWRKID	SYSID	SNTTEVNT	SNTFRTYP	SNTFRNAM	
	SNTGEVCC	SNTSEVCC	SNTGPID	SNTGAID	YEAR	
	WEEK	ZONE	HOUR			
MONTHS	NETWRKID	SYSID	SNTTEVNT	SNTFRTYP	SNTFRNAM	
	SNTGEVCC	SNTSEVCC	SNTGPID	SNTGAID	YEAR	
	MONTH	ZONE				
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-10. SNTLNF Timespan Granularity Chart

5.2.10.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

X - DETAIL
D - DAYS
W - WEEKS
M - MONTHS
Y - YEARS
T - TABLE AREA
. - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XDW...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	SNTFRNAM	- Failing Resource Name
XDWM..E	SNTFRTYP	- Failing Resource Type
XDWM..E	SNTGAID	- Generic Alert ID

XDWM..E SNTGEVCC - General Event Cause Code
XDWM..E SNTGPID - Generic Product ID
XDWM..E SNTSEVCC - Specific Event Cause Code
XDWM..E SNTTEVNT - Type of Event
XDWM..E SYSID - System Identifier
XDW...E WEEK - Week of Year
XDWM..E YEAR - Year of Century
XDWM..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
XDWM..E ENDTS - End Time Stamp
XDWM.. MICSVER - CA MICS Version Number
XDWM..E PRODUCT - Network Product (Source) Name
XDWM.. PRODVRL - Product Version and Release
XD....E SNTACTCD - Event Action Code
XD....E SNTBLKCD - Event Block Code
XDWM..E SNTCMLI - Complex Link Indicator (Y or N)
X.....E SNTCNTMK - Record Content Mask
XDWM..E SNTCODPT - Generic Code Points 2 to 5
XDWM..E SNTDMNAM - Domain Name
XDW...E SNTDQFR1 - Detail Qualifier 1
XDW...E SNTDQFR2 - Detail Qualifier 2
XDW...E SNTDQFR3 - Detail Qualifier 3
XDWM..E SNTERRDS - Error Description: Probable Cause
XDWM..E SNTEVETS - Event Time Stamp
XDWM..E SNTERTY - Event Resource Type
XDW...E SNTFRNM1 - Resource Level Name 1
XDW...E SNTFRNM2 - Resource Level Name 2
XDW...E SNTFRNM3 - Resource Level Name 3
XDW...E SNTFRNM4 - Resource Level Name 4
XDW...E SNTFRNM5 - Resource Level Name 5
XDW...E SNTFRTY1 - Resource Level Type 1
XDW...E SNTFRTY2 - Resource Level Type 2
XDW...E SNTFRTY3 - Resource Level Type 3
XDW...E SNTFRTY4 - Resource Level Type 4
XDW...E SNTFRTY5 - Resource Level Type 5
XDWM..E SNTGADSC - Generic Alert Description
X.....E SNTGFLAG - Generic Flags
XDWM..E SNTNRALT - Number of Alerts
XDWM..E SNTNREVT - Number of Events
XDWM..E SNTNRGEV - Number of Generic Events
XDWM..E SNTTERR - Total Temporary Errors
XDWM..E SNTTTRFC - Total Traffic
XDWM..E SNT1PRBC - Generic First Probable Cause
XDWM..E STARTTS - Start Time Stamp
XDWM.. TMOFFSET - Time Offset

Retained Data Elements

X.....E LNFDMAC - MAC Address of Downstream Member
X.....E LNFLCMAC - Local MAC Address
X..... LNFRROUTE - Routing Information
X.....E LNFRMAC - Remote MAC Address
X.....E LNFUPMAC - MAC Address of Upstream Member
X.....E LNFIMACA - Single MAC Address
X.....E LNFIMACN - Single MAC Name

5.2.10.3 Usage Considerations

This section identifies the special considerations or techniques related to using the SNTLNF File. Additionally, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As the files granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEK should not be used in MONTHS.
2. The following data elements are user-defined. The value in each is dependent on user-selected options or user supplied SAS code:
 - o NETWRKID - Network Identifier. A one to 8-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - Time offset applied to the data in the file. The user can associate a time offset with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. Time offset is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

3. The following data elements lose significance once summarization has been performed. These data elements should only be referenced when the last observed value in a summarization interval is significant.

NPDAVRRL - NPDA Version/Release

TMOFFSET - Time Offset

SNTCMPLI - Complex Link Indicator (Y or N)

Retrieval Examples

1. Produce a count of the number of NPDA Events by resource type. Use last week's data.

```
PROC FREQ DATA=&PSNTW..SNTLNF01;  
  TABLES SNTFRTYP / NOROW NOCUM NOCOL;  
  WEIGHT SNTNREVT;
```

2. Produce a report showing the 50 resources having the highest incident rate for NPDA Event Alerts. Use last month's data.

```
PROC SORT DATA=&PSNTM..SNTLNF01 OUT=WKLNF;  
  BY DESCENDING SNTNRALT;
```

```
OPTIONS OBS=50;
```

```
PROC PRINT DATA=WKLNF;  
  ID SNTFRTYP SNTFRNAM;  
  VAR SNTNREVT SNTNRALT SNTERRDS;
```

5.2.11 NPDA Generic Alert File (SNTGAF)

The NPDA Generic Alert File (SNTGAF) quantifies, by failing resource name and type, the total number of generic events and alerts for all system and network resources, excluding those for LAN resources. The file is derived from the NetView Hardware Monitor External Log record.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.11.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

+-----+-----+ Timespan Level of Data Granularity +-----+-----+						
	DETAIL	NETWRKID	SYSID	SNTTEVNT	SNTFRTYP	SNTFRNAM
		SNTGPID	SNTGAID	YEAR	MONTH	DAY
		HOUR	ENDTS			
	DAYS	NETWRKID	SYSID	SNTTEVNT	SNTFRTYP	SNTFRNAM
		SNTGPID	SNTGAID	YEAR	MONTH	DAY
		HOUR				
	WEEKS	NETWRKID	SYSID	SNTTEVNT	SNTFRTYP	SNTFRNAM
		SNTGPID	SNTGAID	YEAR	WEEK	ZONE
		HOUR				
	MONTHS	NETWRKID	SYSID	SNTTEVNT	SNTFRTYP	SNTFRNAM
		SNTGPID	SNTGAID	YEAR	MONTH	ZONE
	YEARS	N/A				
+-----+-----+						
	TABLES	N/A				
+-----+-----+						

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=DEFAult option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-11. SNTGAF Timespan Granularity Chart

5.2.11.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XDW...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	SNTFRNAM	- Failing Resource Name
XDWM..E	SNTFRTYP	- Failing Resource Type

XDW..E SNTGAID - Generic Alert ID
XDW..E SNTGPID - Generic Product ID
XDW..E SNTTEVNT - Type of Event
XDW..E SYSID - System Identifier
XDW...E WEEK - Week of Year
XDW..E YEAR - Year of Century
XDW..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
XDW..E ENDTS - End Time Stamp
XDW.. MICSVER - CA MICS Version Number
XDW..E PRODUCT - Network Product (Source) Name
XDW.. PRODVRRL - Product Version and Release
XDW..E SNTCMPLI - Complex Link Indicator (Y or N)
X.....E SNTCNTMK - Record Content Mask
XDW..E SNTCODPT - Generic Code Points 2 to 5
XDW..E SNTDMNAM - Domain Name
XDW..E SNTDEVTS - Event Time Stamp
XDW...E SNTFRNM1 - Resource Level Name 1
XDW...E SNTFRNM2 - Resource Level Name 2
XDW...E SNTFRNM3 - Resource Level Name 3
XDW...E SNTFRNM4 - Resource Level Name 4
XDW...E SNTFRNM5 - Resource Level Name 5
XDW...E SNTFRTY1 - Resource Level Type 1
XDW...E SNTFRTY2 - Resource Level Type 2
XDW...E SNTFRTY3 - Resource Level Type 3
XDW...E SNTFRTY4 - Resource Level Type 4
XDW...E SNTFRTY5 - Resource Level Type 5
XDW..E SNTGADSC - Generic Alert Description
X.....E SNTGFLAG - Generic Flags
XDW..E SNTNRALT - Number of Alerts
XDW..E SNTNRGEV - Number of Generic Events
XDW..E SNT1PRBC - Generic First Probable Cause
XDW..E STARTTS - Start Time Stamp
XDW..E TMOFFSET - Time Offset

5.2.11.3 Usage Considerations

This section identifies the special considerations or techniques related to using the SNTGAF File. Additionally, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As the files granularity increases in higher timespans certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEK should not be used in MONTHS.
2. The following data elements are user-defined. The value in each is dependent on user-selected options or user supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - Time offset applied to the data in the file. The user can associate a time offset with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. Time offset is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

3. The following data elements lose significance once summarization has been performed. These data elements should only be referenced when the last observed value in a summarization interval is significant.

NPDAVRRL - NPDA Version/Release
TMOFFSET - Time Offset
SNTCMPLI - Complex Link Indicator (Y or N)

Retrieval Examples

1. Produce a count of the number of NPDA Generic Events by resource type. Use last week's data.

```
PROC FREQ DATA=&PSNTW..SNTGAF01;  
  TABLES SNTFRTYP / NOROW NOCUM NOCOL;  
  WEIGHT SNTNRGEV;
```

2. Produce a report showing the 50 resources having the highest incident rate for NPDA Generic Alerts. Use last month's data.

```
PROC SORT DATA=&PSNTM..SNTGAF01 OUT=WKGAF;  
  BY DESCENDING SNTNRALT;  
  
OPTIONS OBS=50;  
  
PROC PRINT DATA=WKGAF;  
  ID SNTFRTYP SNTFRNAM;  
  VAR SNTNRGEV SNTNRALT SNTGADSC;
```

5.2.12 NLDM Service File (SNTNSV)

The NLDM Service File (SNTNSV) quantifies service received, including average response times and response distribution percentages, organized by site-defined performance classes. The file is derived from the NetView Session Monitor/NLDM External Log record or the CA NetMaster NTS SMF record.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.12.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	NSVPCLSS	YEAR	MONTH	
	DAY	HOUR	ENDTS			
DAYS	NETWRKID	SYSID	NSVPCLSS	YEAR	MONTH	
	DAY	HOUR				
WEEKS	NETWRKID	SYSID	NSVPCLSS	YEAR	WEEK	
	ZONE	HOUR				
MONTHS	NETWRKID	SYSID	NSVPCLSS	YEAR	MONTH	
	ZONE					
YEARS	NETWRKID	SYSID	NSVPCLSS	YEAR	ZONE	
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-12. SNTNSV Timespan Granularity Chart

5.2.12.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XDW...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWMY.E	NETWRKID	- Network Identifier
XDWMY.E	NSVPCLSS	- Performance Class
XDWMY.E	SYSID	- System Identifier

XDW...E WEEK - Week of Year
 XDWMY.E YEAR - Year of Century
 XDWMY.E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
 XDWMY. DURATION - Recording Interval Time
 XDWMY.E ENDTS - End Time Stamp
 XDWMY. MICSVER - CA MICS Version Number
 XDWMY. NLDMVRRL - NLDM Version and Release Id
 XDWMY.E NLDLVAL1 - NLDM Response Distribution Limits 1
 XDWMY.E NLDLVAL2 - NLDM Response Distribution Limits 2
 XDWMY.E NLDLVAL3 - NLDM Response Distribution Limits 3
 XDWMY.E NLDLVAL4 - NLDM Response Distribution Limits 4
 XDWMY. PLDOMAIN - PLU Domain Name
 XD....E PLU - Primary Logical Unit
 XD.... PLUSAPU - PLU Subarea Physical Unit
 XDWMY. PRODUCT - Network Product (Source) Name
 XDWMY.E SAMPLES - Number of Samples
 XDWMY. SLDOMAIN - SLU Domain Name
 XD....E SLU - Secondary Logical Unit
 XD.... SLULINK - SLU Link
 XD.... SLUPU - SLU Physical Unit
 XD.... SLUSAPU - SLU Subarea Physical Unit
 XDWMY.E STARTTS - Start Time Stamp
 XDWMY. TMOFFSET - Time Offset

Retained Data Elements

XDWMY.E NSVCNTR - Objective Counter Number
 XDWMY. NSVCOS - Class of Service
 XD.... NSVEXRTE - Explicit Route Number
 XDWMY.E NSVPCOBJ - Objective Percentage
 XDWMY. NSVRDEF - Response Definition
 XDWMY.E NSVROBTM - Objective Response Time
 XD.... NSVRVER - Reverse Explicit Route Number
 XD.... NSVSTYPE - Session Type
 XD.... NSVTRPTY - Transmission Priority
 XD.... NSVVRTE - Virtual Route Number
 XD.... NSVXNET - Cross-network Session

Accumulated Data Elements

XDWMY.E NSVNRROM - Number of Times Resp Obj Met
 XDWMY.E NSVRDST1 - Response Dist Count 1 (Boundary A)
 XDWMY.E NSVRDST2 - Response Dist Count 2 (Boundary B)
 XDWMY.E NSVRDST3 - Response Dist Count 3 (Boundary C)
 XDWMY.E NSVRDST4 - Response Dist Count 4 (Boundary D)

XDWMY.E NSVRDST5 - Response Dist Count 5 (Above A,B,C,D)
XDWMY.E NSVTRESC - Total Response Event Count
XDWMY.E NSVTRSTM - Total Response Time

Derived Data Elements

XDWMY.E NSVAVTM - Average Total Response Time
XDWMY.E NSVPCOBM - Pct of Times Response Obj Met
XDWMY.E NSVPCTR1 - Cum. Pct All Resp Within Limit 1
XDWMY.E NSVPCTR2 - Cum. Pct All Resp Within Limit 2
XDWMY.E NSVPCTR3 - Cum. Pct All Resp Within Limit 3
XDWMY.E NSVPCTR4 - Cum. Pct All Resp Within Limit 4

5.2.12.3 Usage Considerations

This section identifies the special considerations or techniques related to using the SNTNSV File. Additionally, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As the files granularity increases in higher timespans certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEK should not be used in MONTHS.
2. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - Time offset applied to the data in the file. The user can associate a time offset with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. Time offset is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

3. The following data elements lose significance once summarization has been performed. These data elements should only be referenced when the last observed value in a summarization interval is significant.

NLDMVRR - NLDM Version and Release ID
NLDRVAL1 - NLDM Response Distribution Limits 1
NLDRVAL2 - NLDM Response Distribution Limits 2
NLDRVAL3 - NLDM Response Distribution Limits 3
NLDRVAL4 - NLDM Response Distribution Limits 4
PLDOMAIN - PLU Domain Name
PLU - Primary Logical Unit
PLUSAPU - PLU Subarea Physical Unit
SLDOMAIN - SLU Domain Name
SLU - Secondary Logical Unit
SLULINK - SLU Link
SLUPU - SLU Physical Unit
SLUSAPU - SLU Subarea Physical Unit
TMOFFSET - Time Offset
NSVCNTR - Objective Counter Number
NSVCOS - Class of Service
NSVEXRTE - Explicit Route Number
NSVPCOBJ - Objective Percentage
NSVRDEF - Response Definition
NSVROBTM - Objective Response Time
NSVRVER - Reverse Explicit Route Number
NSVSTYPE - Session Type
NSVTRPTY - Transmission Priority
NSVVRTE - Virtual Route Number
NSVXNET - Cross-network Session

Retrieval Examples

1. Assume that the data center response time objectives state that 90% of all total responses must be less than five (5) seconds. Assuming NLDM is parameterized for Performance Class (NSVPCLSS) 'TSO' such that NLDRVAL2 (response time limit bucket 2) is set at 5 seconds, select those sessions not meeting the stated objective. List each session and relevant information.

```
DATA WKFILE;  
  SET &PSNTX..SNTNSV01;  
  IF NSVPCLSS = 'TSO';  
  IF NSVPCTR3 LT 90; /* SELECT LESS THAN 90 % */  
  
PROC PRINT DATA=WKFILE;  
  ID NETWRKID SYSID;
```



```
VAR PLU SLULINK SLU NSVAVTM;
```

2. Produce a report showing a count of terminal (SLUs) by application (PLU) missing their response objectives using today's data.

```
DATA WKNSV;  
SET &PSNTX..SNTNSV01;  
IF NSVNRROM=0; /* =1 IN DETAIL IF OBJ MET */
```

```
PROC FREQ DATA=WKNSV;  
TABLES PLU * SLU / NOROW NOCOL NOCUM;
```

5.2.13 CA NetSpy Application (PLU) File (SNTNSP)

The CA NetSpy Application (PLU) Activity File (SNTNSP) quantifies response time and network traffic (load) statistics by application. The file is derived from the CA NetSpy session monitor SMF record (subtype A) or its VM equivalent.

The source data contains monitor records for only those applications CA NetSpy is directed to monitor.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.13.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Figure 5-13. SNTNSP Timespan Granularity Chart

5.2.13.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

X - DETAIL
 D - DAYS
 W - WEEKS
 M - MONTHS
 Y - YEARS
 T - TABLES AREA
 . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XDW...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	PLU	- Primary Logical Unit
XDWM..E	SYSID	- System Identifier

XDW...E WEEK - Week of Year
XDW..E YEAR - Year of Century
XDW..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
XDW..E DURATION - Recording Interval Time
XDW..E ENDTS - End Time Stamp
XDW..E INTERVLS - Number of Recording Intervals
XDW..E MICSVER - CA MICS Version Number
XDW..E NSPYVER - NetSpy Version/Release Number
XDW..E PLUMSMGR - PLU Multi-Session Manager Flag
XDW..E PRODUCT - Network Product (Source) Name
XDW..E RDSTTYPE - Response Distribution Target Flag
XDW..E STARTTS - Start Time Stamp
XDW..E TMOFFSET - Time Offset

Retained Data Elements

XDW..E NSPACID - Application CID (network address)
XDW..E NSPHSA - Host Subarea Address (VTAM V3)
XDW..E NSPLHRTM - Last Host Response Time
XDW..E NSPLNRTM - Last Network Response Time
X.....E NSPNRSLU - Number of Terminals (SLUs) Monitored
XDW..E NSPNWIDA - Network Identifier for Application
XDW..E NSPRVAL1 - Response Distribution Limit 1
XDW..E NSPRVAL2 - Response Distribution Limit 2
XDW..E NSPRVAL3 - Response Distribution Limit 3
XDW..E NSPRVAL4 - Response Distribution Limit 4
XDW..E NSPXDMN - Cross Domain Flag

Accumulated Data Elements

XDW..E NSPHRSTM - Host Response Time
XDW..E NSPNRBYR - Cumulative Bytes Received
XDW..E NSPNRBYS - Cumulative Bytes Sent
XDW..E NSPNRESC - Network Responses
XDW..E NSPNRNRS - Non-Response Time Measured Bytes Sent
XDW..E NSPNROUT - Number of Outputs
X.....E NSPNRSES - Number of Sessions Monitored
XDW..E NSPNRSTM - Network Response Time (Measured)
XDW..E NSPNRTRI - Number of Transactions (LU62 Sessions)
XDW..E NSPNRTXS - Number of Transactions (# of Inputs)
XDW..E NSPNRURM - Total User Responses Measured (LU62)
XDW..E NSPRDST1 - Response Distribution Count 1
XDW..E NSPRDST2 - Response Distribution Count 2
XDW..E NSPRDST3 - Response Distribution Count 3
XDW..E NSPRDST4 - Response Distribution Count 4

XDWM..E NSPRDST5 - Response Distribution Count 5
XDWM..E NSPTNRUR - Total Number of User Responses Measured
XDWM..E NSPTRESC - Number of Responses

Maximum Data Elements

XDWM..E NSPMXHTM - Maximum Host Response Time
XDWM..E NSPMXNTM - Maximum Network Response Time

Derived Data Elements

XDWM..E NSPAVHTM - Average Host Response Time
XDWM..E NSPAVNTM - Average Network Response Time
XDWM..E NSPAVTTM - Average Total Response Time
XDWM..E NSPCNRTM - Network Response Time (Computed)
XDWM..E NSPPCTR1 - Cum. Pct Total Resp Within Limit 1
XDWM..E NSPPCTR2 - Cum. Pct Total Resp Within Limit 2
XDWM..E NSPPCTR3 - Cum. Pct Total Resp Within Limit 3
XDWM..E NSPPCTR4 - Cum. Pct Total Resp Within Limit 4
XDWM..E NSPTRSTM - Total Response Time

5.2.13.3 Usage Considerations

This section identifies special considerations or techniques related to using the SNTNSP File. In addition, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEKS should not be used in MONTHS.
2. The following data elements are user-defined. The value in each is dependent on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.
3. The following data elements lose significance once

summarization has been performed. These data elements should only be referenced when the last observed value in a summarization interval is significant.

NSPYVER - CA NetSpy Version and Release ID
 TMOFFSET - Time Offset
 NSPACID - Application CID (network address)
 NSPHSA - Host Subarea Address (VTAM V3)
 NSPLHRTM - Last Host Response Time
 NSPLNRTM - Last Network Response Time
 NSPRVAL1 - Response Distribution Limits 1
 NSPRVAL2 - Response Distribution Limits 2
 NSPRVAL3 - Response Distribution Limits 3
 NSPRVAL4 - Response Distribution Limits 4

4. Two CA NetSpy Initialization parameters determine the values for the elements NSPMXHTM, NSPMXNTM, NSPHRSTM, NSPNRSTM, NSPAVHTM, NSPAVNTM, and NSPAVTM. These two parameters are:
 - o HCUTOFF - Host response time cutoff boundary. CA NetSpy discards host response times greater than this boundary. This prevents exceptionally long response times from skewing the average host response time for the application or terminal.
 - o NCUTOFF - Network response time cutoff boundary. CA NetSpy discards network response times greater than this boundary. This prevents exceptionally long response times from skewing the average network response time for the application or terminal.

Retrieval Examples

Chart response time for Primary Logical Unit (PLU) ACICS10.
 Break the chart bars into host and network response time.
 Use yesterday's data.

```
%LET BY = PLU HOUR ;
%LET BREAK = HOUR ;

PROC SORT DATA=&PSNTD..SNTNSP01 OUT=WKNSP;
  BY &BY;

DATA WKNSP;
  SET WKNSP;
  %NSPSUM
RUN;
```

```
DATA WKNSP;  
  SET WKNSP;  
  IF PLU='ACICS10';  
  RESPONSE=NSPAVNTM; TYPESP='NETWORK'; OUTPUT;  
  RESPONSE=NSPAVHTM; TYPESP='HOST '; OUTPUT;  
  
PROC CHART DATA=WKNSP;  
  VBAR HOUR / SUMVAR=RESPONSE  
    SUBGROUP=TYPEESP  
    DISCRETE;RUN;
```

5.2.14 CA NetSpy Terminal (SLU) File (SNTNSS)

The CA NetSpy Terminal (SLU) Activity File (SNTNSS) quantifies response time and network traffic (load) statistics by application-to-terminal session. The file is derived from the CA NetSpy session monitor SMF record (subtypes S, U, or T) or its VM equivalent.

The source data contains monitor records for only those applications CA NetSpy is directed to monitor. In CA NetSpy, a terminal's session can only be monitored for those sessions where the application (PU) is monitored.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.14.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	YEAR	MONTH	DAY	
	HOUR	ENDTS				
DAYS	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	YEAR	MONTH	DAY	
	HOUR					
WEEKS	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	YEAR	WEEK	ZONE	
	HOUR					
MONTHS	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	YEAR	MONTH	ZONE	
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not

is controlled by the complex definition of the DERIVED option.

Figure 5-14. SNTNSS Timespan Granularity Chart

5.2.14.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

X - DETAIL
 D - DAYS
 W - WEEKS
 M - MONTHS
 Y - YEARS
 T - TABLES AREA
 . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XDW...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	SNTACT1	- PRIMARY LOGICAL UNIT(PLU)
XDWM..E	SNTACT2	- SLUSAPU NETV/NPM1.3,SLUSA NPM1.2 OR NSPY

XDW..E SNTACT3 - SLUPU IF NLDM OR NETSPY, SLU IF NPM
XDW..E SNTACT4 - NLDM PERFCLSS, NPM BLANK, NSPY/NAC SLU
XDW..E SNTACT5 - NOT-USED
XDW..E SYSID - System Identifier
XDW...E WEEK - Week of Year
XDW..E YEAR - Year of Century
XDW..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
XDW..E DURATION - Recording Interval Time
XDW..E ENDTS - End Time Stamp
XDW..E INTERVLS - Number of Recording Intervals
XDW..E MICSVER - CA MICS Version Number
X.....E NETGROUP - Network Service Group
XDW..E NSPYVER - NetSpy Version/Release Number
XDW..E PLU - Primary Logical Unit
XDW..E PLUMSMGR - PLU Multi-Session Manager Flag
XDW..E PRODUCT - Network Product (Source) Name
XDW..E RDSTTYPE - Response Distribution Target Flag
XDW..E SLU - Secondary Logical Unit
XD....E SLULINK - SLU Link
XD....E SLUPU - SLU Physical Unit
XDW..E STARTTS - Start Time Stamp
XDW..E TMOFFSET - Time Offset
X.....E USER - User Identification

Retained Data Elements

XDW..E NSSGTARG - Global Resp Dist. Target Flag
XDW..E NSSGVAL1 - Global Response Dist. Limit 1
XDW..E NSSGVAL2 - Global Response Dist. Limit 2
XDW..E NSSGVAL3 - Global Response Dist. Limit 3
XDW..E NSSGVAL4 - Global Response Dist. Limit 4
XDW..E NSSLDEV - Locally Attached Device (Y or N)
XDW..E NSSLHRTM - Last Host Response Time
XDW..E NSSLNRTM - Last Network Response Time
XDW..E NSSLU62F - LU62 Activity Flag
XDW..E NSSNWIDS - Network Identifier for Session LU
XDW..E NSSPRCID - Procedure Correlation ID
XDW..E NSSRVAL1 - Response Distribution Limit 1
XDW..E NSSRVAL2 - Response Distribution Limit 2
XDW..E NSSRVAL3 - Response Distribution Limit 3
XDW..E NSSRVAL4 - Response Distribution Limit 4
XDW..E NSSSTYPE - Terminal Session Rcd Type
XDW..E NSSTCID - Terminal CID (network address)
XDW..E NSSTSA - Terminal Subarea Address (VTAM V3)
XDW..E NSSVIRLU - Virtual Logical Unit Name

XDWM..E NSSVR RTE - Virtual Route Number
 XDWM..E NSSVSESS - Virtual Session Flag

Accumulated Data Elements

XDWM..E NSSCONTM - Session Connect Time
 XDWM..E NSSCOST - Billable Cost
 XDWM..E NSSGDST1 - Global Response Dist. Count 1
 XDWM..E NSSGDST2 - Global Response Dist. Count 2
 XDWM..E NSSGDST3 - Global Response Dist. Count 3
 XDWM..E NSSGDST4 - Global Response Dist. Count 4
 XDWM..E NSSGDST5 - Global Response Dist. Count 5
 XDWM..E NSSHRSTM - Host Response Time
 XDWM..E NSSNRBYR - Cumulative Bytes Received
 XDWM..E NSSNRBYS - Cumulative Bytes Sent
 XDWM..E NSSNRBYT - Cumulative Bytes Total
 XDWM..E NSSNRESC - Network Responses
 XDWM..E NSSNROUT - Number of Outputs
 XDWM..E NSSNRSTM - Network Response Time (Measured)
 XDWM..E NSSNRTRI - Number of Transactions (LU62 Sessions)
 XDWM..E NSSNRURM - Total User Responses Measured
 XDWM..E NSSRDST1 - Response Distribution Count 1
 XDWM..E NSSRDST2 - Response Distribution Count 2
 XDWM..E NSSRDST3 - Response Distribution Count 3
 XDWM..E NSSRDST4 - Response Distribution Count 4
 XDWM..E NSSRDST5 - Response Distribution Count 5
 XDWM..E NSSTRESC - Number of Transactions (# of Inputs)

Maximum Data Elements

XDWM..E NSSMXHTM - Maximum Host Response Time
 XDWM..E NSSMXNTM - Maximum Network Response Time

Derived Data Elements

XDWM..E NSSAVHTM - Average Host Response Time
 XDWM..E NSSAVNTM - Average Network Response Time
 XDWM..E NSSAVTTM - Average Total Response Time
 XDWM..E NSSCNRTM - Network Response Time (Computed)
 XDWM..E NSSPCTG1 - Cum. Pct Within Global Resp Limit 1
 XDWM..E NSSPCTG2 - Cum. Pct Within Global Resp Limit 2
 XDWM..E NSSPCTG3 - Cum. Pct Within Global Resp Limit 3
 XDWM..E NSSPCTG4 - Cum. Pct Within Global Resp Limit 4
 XDWM..E NSSPCTR1 - Cum. Pct Total Resp Within Limit 1
 XDWM..E NSSPCTR2 - Cum. Pct Total Resp Within Limit 2
 XDWM..E NSSPCTR3 - Cum. Pct Total Resp Within Limit 3
 XDWM..E NSSPCTR4 - Cum. Pct Total Resp Within Limit 4
 XDWM..E NSSTRSTM - Total Response Time

5.2.14.3 Usage Considerations

This section identifies special considerations or techniques related to using the SNTNSS File. In addition, a retrieval example is provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEKS should not be used in MONTHS.
2. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.
3. The following data elements lose significance once summarization has been performed. These data elements

should be referenced only when the last observed value in a summarization interval is significant.

NSPYVER - CA NetSpy Version and Release ID
TMOFFSET - TIME OFFSET
NSSLHRTM - Last Host Response Time
NSSLNRTM - Last Network Response Time
NSSRVAL1 - Response Distribution Limit 1
NSSRVAL2 - Response Distribution Limit 2
NSSRVAL3 - Response Distribution Limit 3
NSSRVAL4 - Response Distribution Limit 4
NSSTCID - Terminal CID (network address)
NSS TSA - Terminal Subarea Address (VTAM V3)
NSSVRTE - Virtual Route Number

4. User selection of CA NetSpy options determine what terminal information is contained in the source data and what is omitted. CA NetSpy collects information for terminals only when they are in session with applications that CA NetSpy has been directed to monitor.

For example, CA NetSpy has been requested to monitor only TSO. During the day, a terminal is in session with TSO and CICS. In this case, only the terminal's sessions with TSO are contained in the source data. Moreover, CA NetSpy can be directed to collect on all terminals when they are in session with an application or on only a subset of these terminals. In the latter case, summarizing the observations for the terminals by PLU would present an incomplete picture of that PLU's workload and performance.

5. Two CA NetSpy Initialization parameters determine the values for the elements NSSMXHTM, NSSMXNTM, NSSHRSTM, NSSNRSTM, NSSAVHTM, NSSAVNTM, and NSSAVTTM. These two parameters are:
 - o HCUTOFF - Host response time cutoff boundary. CA NetSpy discards host response times greater than this boundary. This prevents exceptionally long response times from skewing the average host response time for the application or terminal.
 - o NCUTOFF - Network response time cutoff boundary. CA NetSpy discards network response times greater than this boundary. This prevents exceptionally long response times from skewing the average network response time for the application or terminal.

6. The element USER will have a missing value unless you define a value for the CA NetSpy Initialization parameter USRIDUPD. This parameter specifies the interval during which CA NetSpy searches for all TSO user IDs that have logged on to a particular terminal during a measurement interval. If you do not specify a value for USRIDUPD, CA NetSpy will not search for TSO user IDs.

Retrieval Example

Assume that CA NetSpy is requested to collect data for all terminals in session with TSO. Assume also that the data center response time objectives state that 90% of total responses must be less than four (4) seconds for TSO, and that initialization parameters are defined so that response distribution limit 3 (service level target 3) is set at four seconds for TSO. Select those sessions not meeting the service-level target. List each secondary session partner and relevant information.

In the example below, the session secondary partner, generally the terminal name, is contained in the SLU data element. The NSSAVTTM data element contains the average total response time for the terminal and NSSPCTR3 contains the actual percentage of transactions with less than four (4) seconds total response time.

```
DATA WKFILE;
  SET &PSNTX..SNTNSS01;
  IF PLU = 'TSO';
  IF NSSPCTR3 LT 90; /* SELECT LESS THAN 90 % */

PROC PRINT DATA=WKFILE;
  ID NETWRKID SYSID;
  VAR PLU SLU NSSAVTTM NSSPCTR3;
```


5.2.15 CA NetSpy Virtual Route Activity File (SNTNVR)

The CA NetSpy Virtual Route Activity File (SNTNVR) quantifies network traffic and response time statistics by SNA virtual route. The file is derived from the CA NetSpy session monitor SMF record (subtype V) or its VM equivalent.

The source data contains monitor records for only those virtual routes CA NetSpy is directed to monitor. The response time information in this file reflects the response time within only the backbone portion of the network path and excludes any additional delay imposed by the boundary portion of the network path.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.15.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan		Level of Data Granularity				
DETAIL	NETWRKID	SYSID	NVRHSA	NVRDSA	NVRVRRTE	
	NVRTRPTY	YEAR	MONTH	DAY	HOUR	
	ENDTS					
DAYS	NETWRKID	SYSID	NVRHSA	NVRDSA	NVRVRRTE	
	NVRTRPTY	YEAR	MONTH	DAY	HOUR	
WEEKS	NETWRKID	SYSID	NVRHSA	NVRDSA	NVRVRRTE	
	NVRTRPTY	YEAR	WEEK	ZONE	HOUR	
MONTHS	NETWRKID	SYSID	NVRHSA	NVRDSA	NVRVRRTE	
	NVRTRPTY	YEAR	MONTH	ZONE		
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=DEFAult option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-15. SNTNVR Timespan Granularity Chart

5.2.15.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XDW...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	NVRDSA	- Destination Subarea Address
XDWM..E	NVRHSA	- Host Subarea Address
XDWM..E	NVRTRPTY	- Transmission Priority

XDWM..E NVRVRTE - Virtual Route Number
 XDWM..E SYSID - System Identifier
 XDWM..E WEEK - Week of Year
 XDWM..E YEAR - Year of Century
 XDWM..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
 XDWM..E DURATION - Recording Interval Time
 XDWM..E ENDTS - End Time Stamp
 XDWM..E INTERVLS - Number of Recording Intervals
 XDWM..E MICSVER - CA MICS Version Number
 XDWM..E NSPYVER - NetSpy Version/Release Number
 XDWM..E PRODUCT - Network Product (Source) Name
 XDWM..E STARTTS - Start Time Stamp
 XDWM..E TMOFFSET - Time Offset

Retained Data Elements

X..... NVRBLKTM - Time VR Became Blocked
 X..... NVRINTWS - Current Window Size at Interval
 X.....E NVRPRTM - Time of Last Pacing Request
 X.....E NVRSTAT - Virtual Route Status

Accumulated Data Elements

XDWM..E NVRNRBYR - Cumulative Bytes Received
 XDWM..E NVRNRBYS - Cumulative Bytes Sent
 XDWM..E NVRNRESC - Network Responses (Measured)
 XDWM..E NVRNRMOP - Measured Outbound PIUs
 XDWM..E NVRNRMPR - Measured Pacing Requests
 XDWM..E NVRNRPHB - Number of PIUs Held or Blocked
 XDWM..E NVRNRPWC - Pacing Window Count
 XDWM..E NVRNRSES - Number of LU-LU Sessions on VR
 XDWM..E NVRNRSTM - Network Response Time (Measured)
 XDWM..E NVRNRTIP - Total Inbound PIUs
 XDWM..E NVRNRTOP - Total Outbound PIUs
 XDWM..E NVRTHLTM - Cumulative Time VR Held/Blocked

Minimum Data Elements

XDWM..E NVRMNWS - Minimum Window Size Observed

Maximum Data Elements

XDWM..E NVRMXWS - Maximum Window Size Observed

Derived Data Elements

XDM..E NVRAVNTM - Average Network Response Time
XDM..E NVRAVPL - Average Outbound PIU Length
XDM..E NVRAVPWS - Average Pacing Window Size
XDM..E NVRPCTHL - Percentage of Time VR Held/Blocked

5.2.15.3 Usage Considerations

This section identifies special considerations or techniques related to using the SNTNVR File. In addition, we provide a retrieval example to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diiiit, where d is the database identifier, iii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Exercise care in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEKS should not be used in MONTHS.
2. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID--Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7 of this guide.
 - o TMOFFSET--TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7 of this guide.
3. The following data elements lose significance once summarization has been performed. Reference these data

elements only when the last observed value in a summarization interval is significant.

NSPYVER - CA NetSpy Version and Release ID
TMOFFSET - TIME OFFSET

4. User selection of CA NetSpy options determine what terminal information is contained in the source data and what is omitted.

Retrieval Example

Assume that complaints about poor response time have been received from a group of end users. After examining information from the CA NetSpy Terminal File (SNTNSS), you determine that there is excessive delay in the network and identify virtual route 1 between subareas 1 and 27 as being the virtual route traversed by the problem sessions. You are now interested in determining whether the excessive network delay is occurring in the backbone or the boundary portion of the network.

The following example will list the average backbone response times for virtual route 1 between subareas 1 and 27 for each CA NetSpy monitor interval during the previous day. From this information, you will be able to determine whether the excessive delay is occurring in the backbone network. If it is not, then you have to focus your attention on the boundary segment of the network.

```
DATA WKFILE;  
  SET &PSNTX..SNTNVR01;  
  IF NVRHSA EQ 1 AND NVRDSA EQ 27 AND NVRVR RTE EQ 1;  
  
PROC PRINT DATA=WKFILE;  
  ID NVRHSA NVRDSA NVRVR RTE;  
  VAR NVRVNTM NVRNRESC NVRNRBYS NVRNR TOP;
```


5.2.16 NCP Network Accounting File (SNTNAC)

The NCP Network Accounting File (SNTNAC) quantifies network traffic statistics by user-defined account codes. This file is derived from either the CA NetSpy network accounting record or the NPM SMF type 28 record (Network Session Accounting/Network Gateway Accounting).

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.16.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	FUNCTION	NACCOLPT	SNTACT1	
	SNTACT2	SNTACT3	SNTACT4	SNTACT5	YEAR	
	MONTH	DAY	HOUR	ENDTS		
DAYS	NETWRKID	SYSID	FUNCTION	NACCOLPT	SNTACT1	
	SNTACT2	SNTACT3	SNTACT4	SNTACT5	YEAR	
	MONTH	DAY	HOUR			
WEEKS	NETWRKID	SYSID	FUNCTION	NACCOLPT	SNTACT1	
	SNTACT2	SNTACT3	SNTACT4	SNTACT5	YEAR	
	WEEK	ZONE	HOUR			
MONTHS	NETWRKID	SYSID	FUNCTION	NACCOLPT	SNTACT1	
	SNTACT2	SNTACT3	SNTACT4	SNTACT5	YEAR	
	MONTH	ZONE				
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not

is controlled by the complex definition of the
DERIVED option.

Figure 5-16. SNTNAC Timespan Granularity Chart

5.2.16.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XDWM..E	FUNCTION	- Product Function
XDW...E	HOURL	- Hour of Day
XDWM..E	MONTH	- Month of Year
XDWM..E	NACCOLPT	- MCP Collection Point (P or S)
XDWM..E	NETWRKID	- Network Identifier

XDWM..E SNTACT1 - PRIMARY LOGICAL UNIT(PLU)
 XDWM..E SNTACT2 - SLUSAPU NETV/NPM1.3,SLUSA NPM1.2 OR NSPY
 XDWM..E SNTACT3 - SLUPU IF NLDM OR NETSPY, SLU IF NPM
 XDWM..E SNTACT4 - NLDM PERFCLSS, NPM BLANK, NSPY/NAC SLU
 XDWM..E SNTACT5 - NOT-USED
 XDWM..E SYSID - System Identifier
 XDWM..E WEEK - Week of Year
 XDWM..E YEAR - Year of Century
 XDWM..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
 XDWM..E ENDTS - End Time Stamp
 XDWM.. MICSVER - CA MICS Version Number
 X.....E NETGROUP - Network Service Group
 XD....E PLU - Primary Logical Unit
 XD....E PLUNETID - PLU Network Id
 XD....E PLUSA - Primary Logical Unit Subarea
 XD....E PLUSAPU - PLU Subarea Physical Unit
 XDWM..E PRODUCT - Network Product (Source) Name
 XDWM..E PRODVRL - Product Version and Release
 XDWM..E SAMPLES - Number of Samples
 X.....E SESTYPE - Session Type
 XD....E SLU - Secondary Logical Unit
 XD....E SLULINK - SLU Link
 XD....E SLUNETID - SLU Network Id
 XD....E SLUPU - SLU Physical Unit
 XD....E SLUSA - Secondary Logical Unit Subarea
 XD....E SLUSAPU - SLU Subarea Physical Unit
 XDWM..E STARTTS - Start Time Stamp
 XDWM.. TMOFFSET - Time Offset
 X.....E USESSIDC - Unique Session ID (Character)

Retained Data Elements

X.....E NACAKPLU - ALIAS PLU Name (NGA)
 X.....E NACAISLU - ALIAS SLU Name (NGA)
 X.....E NACANPLU - Adjacent NETID PLU Side (NGA)
 X.....E NACANSLU - Adjacent NETID SLU Side (NGA)
 X.....E NACCLNCP - Collector NCP Name
 X.....E NACCLNET - Collector NCP NETID
 X.....E NACCPNAM - Network Qualified CP Name
 X.....E NACIEXRT - Inbound Explicit Route Number
 X.....E NACLDEV - Locally Attached Device Flag
 X.....E NACNPMTS - Time Stamp When NPM Received
 X.....E NACOEXRT - Outbound Explicit Route Number
 X.....E NACOVFL - NGA/NSA Data Overflow Flag
 XDWM..E NACPVAL1 - PIU Distribution Limit 1

XDW..E NACPVAL2 - PIU Distribution Limit 2
XDW..E NACPVAL3 - PIU Distribution Limit 3
XDW..E NACPVAL4 - PIU Distribution Limit 4
XDW..E NACPVAL5 - PIU Distribution Limit 5
XDW..E NACPVAL6 - PIU Distribution Limit 6
X....E NACRSTYP - Record Subtype (S, E, or I)
X....E NACSEETS - Session End Time Stamp
X....E NACSEQNO - NSA/NGA Sequence Number
X....E NACSESTS - Session Start Time Stamp
X....E NACSISTS - Session Interval Start Time Stamp
X....E NACTG - Transmission Group
X....E NACTRPTY - Transmission Priority
X....E NACVRTE - Virtual Route Number
XD....E NACXDMN - Cross-domain Session (Y, N, or U)
XD....E NACXNET - Cross-network Session (Y, N or U)

Accumulated Data Elements

XDW..E NACCONTM - Connect Time
XDW..E NACCOST - Billable Cost
XDW..E NACNMSES - Number Of Sessions
XDW..E NACNRCBR - Number Control PIU Bytes Received
XDW..E NACNRCBS - Number Control PIU Bytes Sent
XDW..E NACNRCPR - Number Control PIUs Received
XDW..E NACNRCPS - Number Control PIUs Sent
XDW..E NACNRTBR - Number Text PIU Bytes Received
XDW..E NACNRTBS - Number Text PIU Bytes Sent
XDW..E NACNRTPR - Number Text PIUs Received
XDW..E NACNRTPS - Number Text PIUs Sent
XDW..E NACRDST1 - PIU Rec'd Dist Count 1
XDW..E NACRDST2 - PIU Rec'd Dist Count 2
XDW..E NACRDST3 - PIU Rec'd Dist Count 3
XDW..E NACRDST4 - PIU Rec'd Dist Count 4
XDW..E NACRDST5 - PIU Rec'd Dist Count 5
XDW..E NACRDST6 - PIU Rec'd Dist Count 6
XDW..E NACRDST7 - PIU Rec'd Dist Count 7
XDW..E NACSDST1 - PIU Sent Dist Count 1
XDW..E NACSDST2 - PIU Sent Dist Count 2
XDW..E NACSDST3 - PIU Sent Dist Count 3
XDW..E NACSDST4 - PIU Sent Dist Count 4
XDW..E NACSDST5 - PIU Sent Dist Count 5
XDW..E NACSDST6 - PIU Sent Dist Count 6
XDW..E NACSDST7 - PIU Sent Dist Count 7

Derived Data Elements

XDW..E NACAVCPR - Average Control PIU Received
XDW..E NACAVCPS - Average Control PIU Sent
XDW..E NACAVTPR - Average Text PIU Received

XDWM..E NACAVTPS - Average Text PIU Sent
XDWM..E NACNRTBY - Total Number of Bytes Transmitted
XDWM..E NACNRTPI - Total Number of PIUs Transmitted

5.2.16.3 Usage Considerations

This section identifies special considerations or techniques related to using the SNTNAC File. In addition, a retrieval example is provided to facilitate the use of this file.

CA MICS network session accounting/network gateway accounting supports the following versions of CA NetSpy, IBM Tivoli NetView Performance Monitor (NPM), and Network Control Program (NCP), or higher:

- o CA NetSpy Release 6.0 and later
- o NPM Version 2 and later
- o ACF/NCP Version 5 Release 2.1 and later

To prevent potentially serious problems with missing or duplicate data, do NOT use versions, releases, or revisions previous to those specified above.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEKS should not be used in MONTHS.
2. Avoid collecting redundant network session accounting and network gateway accounting data from either NPM or CA NetSpy. This is especially important if you input this data into the CA MICS Accounting and Chargeback product. The following SNTNAC elements can assist you in detecting

redundant data:

NACCOLPT - NCP Collection Point
FUNCTION - Product Function
NACANPLU - Adjacent NETID PLU Side (NGA)
NACANSLU - Adjacent NETID SLU Side (NGA)
USESSIDC - Unique Session ID

An example of redundant data collection occurs when multiple gateway NCPs are traversed by a terminal to application session and each of these NCPs collects gateway accounting data for that session. In this case, the redundant data can be detected by the presence of multiple observations in the DETAIL timespan with identical Unique Session IDs, but different values for Adjacent NETID PLU Side or Adjacent NETID SLU Side. Refer to Section 8.1.3.3 of this guide, Redundant Information Issues, for further information on how to detect and eliminate duplicate network accounting data.

3. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID--Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7 of this guide.
 - o TMOFFSET--TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7 of this guide.
4. The following data elements lose significance once summarization has been performed, unless they are used in the summarization sequence as a result of being included in one of the accounting fields (i.e., SNTACT1, SNTACT2, etc.).
 - ACTLDEV - Locally Attached Device (Y or N)
 - ACTXDMN - Cross-Domain Session (Y or N)
 - ACTXNET - Cross-Network Session (Y or N)
 - NETGROUP - Network Service Group

PLU - Primary Logical Unit
SAMPLES - Number of Samples
SLU - Secondary Logical Unit
SLULINK - SLU Link
SLUSAPU - SLU Subarea Physical Unit
TMOFFSET - TIME OFFSET

Retrieval Example

Report total traffic volumes and connect time for PLU for yesterday. This example is designed for a site that has defined SNTACT1 as PLU in sharedprefix.MICS.PARMS(SNTACRT). If your site has set a different account code for PLU, for example SNTACT2, change all references to SNTACT1 to the account code your site has defined as PLU.

```
/* SET THE BY AND BREAK SUMMARY MACROS */
%LET BY = NETWRKID SYSID SNTACT1;
%LET BREAK = SNTACT1;

PROC SORT DATA=&PSNTD..SNTNAC01 OUT=SORTED;BY &BY;
RUN;

DATA SUMMED (RENAME=(NACCONTM=CONNECT
                    NACNRTBY=BYTES NACNRTPI=PIUS));
SET SORTED;
%NSCSUM;          /* SUM THE DATA */
RUN;

DATA SUMMED;
SET SUMMED;
IF 9 GE HOUR LE 17; /* SELECT PRIME SHIFT */

PROC PRINT; VAR PLU CONNECT BYTES PIUS;
TITLE 'DAYS SNTNAC01, PRIME SHIFT PLU STATISTICS';
RUN;
```

5.2.17 NCP Line Processor Activity File (SNTNLP)

The NCP Line Processor Activity File (SNTNLP) contains data that quantifies NCP 3746 model 900 line processor activity. The data is found in NPM records (SMF28NAC), subtype 16, at sites using NCP 3746-900 processors.

The file is derived from NPM or CA NetSpy running on z/OS or VM systems.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.17.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	NCPNAME	YEAR	MONTH	
	DAY	HOUR	ENDTS			
DAYS	NETWRKID	SYSID	NCPNAME	YEAR	MONTH	
	DAY	HOUR				
WEEKS	NETWRKID	SYSID	NCPNAME	YEAR	WEEK	
	ZONE	HOUR				
MONTHS	NETWRKID	SYSID	NCPNAME	YEAR	MONTH	
	ZONE					
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=DEFAult option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-17. SNTNLP Timespan Granularity Chart

5.2.17.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XDW...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWM..E	NCPNAME	- Network Ctl Program Name
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	SYSID	- System Identifier

XDW...E WEEK - Week of Year
 XDW..E YEAR - Year of Century
 XDW..E ZONE - Time Zone

Common Data Elements

XDW..E DATATYPE - Type of Data Contained in Observation
 XD....E DAYNAME - Name of Day of Week
 XDW..E DURATION - Recording Interval Time
 XDW..E ENDTS - End Time Stamp
 XDW..E INTERVLS - Number of Recording Intervals
 XDW.. MICSVER - CA MICS Version Number
 XDW.. NETNAME - Resource Network Name
 XDW..E NPMTMAOT - Actual Observation Time
 XDW.. NPMTSEIS - Expected Interval Time
 XDW.. NPMTSFRU - Forward RU Send Time
 XDW.. NPMTSLOG - Time Record Logged To SMF
 XDW..E NPMVRL - NPM Version/Release Number
 XDW..E PLUNETID - PLU Network Id
 XDW..E PRODUCT - Network Product (Source) Name
 XDW.. RESNAME - Resource Generic Name
 XDW..E STARTTS - Start Time Stamp
 XDW.. TMOFFSET - Time Offset

Retained Data Elements

X..... NLPLPT1 - 3746-900 Line Processor 1 Type
 X..... NLPLPT10 - 3746-900 Line Processor 10 Type
 X..... NLPLPT11 - 3746-900 Line Processor 11 Type
 X..... NLPLPT12 - 3746-900 Line Processor 12 Type
 X..... NLPLPT13 - 3746-900 Line Processor 13 Type
 X..... NLPLPT14 - 3746-900 Line Processor 14 Type
 X..... NLPLPT15 - 3746-900 Line Processor 15 Type
 X..... NLPLPT16 - 3746-900 Line Processor 16 Type
 X..... NLPLPT17 - 3746-900 Line Processor 17 Type
 X..... NLPLPT18 - 3746-900 Line Processor 18 Type
 X..... NLPLPT2 - 3746-900 Line Processor 2 Type
 X..... NLPLPT3 - 3746-900 Line Processor 3 Type
 X..... NLPLPT4 - 3746-900 Line Processor 4 Type
 X..... NLPLPT5 - 3746-900 Line Processor 5 Type
 X..... NLPLPT6 - 3746-900 Line Processor 6 Type
 X..... NLPLPT7 - 3746-900 Line Processor 7 Type
 X..... NLPLPT8 - 3746-900 Line Processor 8 Type
 X..... NLPLPT9 - 3746-900 Line Processor 9 Type

Minimum Data Elements

X..... NLPBSU1 - 3746-900 Line Processor 1 BUFF Util.
 X..... NLPBSU10 - 3746-900 Line Processor 10 BUFF Util.

X.....	NLPBSU11	- 3746-900	Line Processor 11	BUFF Util.
X.....	NLPBSU12	- 3746-900	Line Processor 12	BUFF Util.
X.....	NLPBSU13	- 3746-900	Line Processor 13	BUFF Util.
X.....	NLPBSU14	- 3746-900	Line Processor 14	BUFF Util.
X.....	NLPBSU15	- 3746-900	Line Processor 15	BUFF Util.
X.....	NLPBSU16	- 3746-900	Line Processor 16	BUFF Util.
X.....	NLPBSU17	- 3746-900	Line Processor 17	BUFF Util.
X.....	NLPBSU18	- 3746-900	Line Processor 18	BUFF Util.
X.....	NLPBSU2	- 3746-900	Line Processor 2	BUFF Util.
X.....	NLPBSU3	- 3746-900	Line Processor 3	BUFF Util.
X.....	NLPBSU4	- 3746-900	Line Processor 4	BUFF Util.
X.....	NLPBSU5	- 3746-900	Line Processor 5	BUFF Util.
X.....	NLPBSU6	- 3746-900	Line Processor 6	BUFF Util.
X.....	NLPBSU7	- 3746-900	Line Processor 7	BUFF Util.
X.....	NLPBSU8	- 3746-900	Line Processor 8	BUFF Util.
X.....	NLPBSU9	- 3746-900	Line Processor 9	BUFF Util.
X.....	NLPLPU1	- 3746-900	Line Processor 1	CPU Util.
X.....	NLPLPU10	- 3746-900	Line Processor 10	CPU Util.
X.....	NLPLPU11	- 3746-900	Line Processor 11	CPU Util.
X.....	NLPLPU12	- 3746-900	Line Processor 12	CPU Util.
X.....	NLPLPU13	- 3746-900	Line Processor 13	CPU Util.
X.....	NLPLPU14	- 3746-900	Line Processor 14	CPU Util.
X.....	NLPLPU15	- 3746-900	Line Processor 15	CPU Util.
X.....	NLPLPU16	- 3746-900	Line Processor 16	CPU Util.
X.....	NLPLPU17	- 3746-900	Line Processor 17	CPU Util.
X.....	NLPLPU18	- 3746-900	Line Processor 18	CPU Util.
X.....	NLPLPU2	- 3746-900	Line Processor 2	CPU Util.
X.....	NLPLPU3	- 3746-900	Line Processor 3	CPU Util.
X.....	NLPLPU4	- 3746-900	Line Processor 4	CPU Util.
X.....	NLPLPU5	- 3746-900	Line Processor 5	CPU Util.
X.....	NLPLPU6	- 3746-900	Line Processor 6	CPU Util.
X.....	NLPLPU7	- 3746-900	Line Processor 7	CPU Util.
X.....	NLPLPU8	- 3746-900	Line Processor 8	CPU Util.
X.....	NLPLPU9	- 3746-900	Line Processor 9	CPU Util.
X.....	NLPPSU1	- 3746-900	Line Prosr 1	Fast Pgm Stg Util
X.....	NLPPSU10	- 3746-900	Line Prosr 10	Fast Pgm Stg Util
X.....	NLPPSU11	- 3746-900	Line Prosr 11	Fast Pgm Stg Util
X.....	NLPPSU12	- 3746-900	Line Prosr 12	Fast Pgm Stg Util
X.....	NLPPSU13	- 3746-900	Line Prosr 13	Fast Pgm Stg Util
X.....	NLPPSU14	- 3746-900	Line Prosr 14	Fast Pgm Stg Util
X.....	NLPPSU15	- 3746-900	Line Prosr 15	Fast Pgm Stg Util
X.....	NLPPSU16	- 3746-900	Line Prosr 16	Fast Pgm Stg Util
X.....	NLPPSU17	- 3746-900	Line Prosr 17	Fast Pgm Stg Util
X.....	NLPPSU18	- 3746-900	Line Prosr 18	Fast Pgm Stg Util
X.....	NLPPSU2	- 3746-900	Line Prosr 2	Fast Pgm Stg Util
X.....	NLPPSU3	- 3746-900	Line Prosr 3	Fast Pgm Stg Util
X.....	NLPPSU4	- 3746-900	Line Prosr 4	Fast Pgm Stg Util
X.....	NLPPSU5	- 3746-900	Line Prosr 5	Fast Pgm Stg Util
X.....	NLPPSU6	- 3746-900	Line Prosr 6	Fast Pgm Stg Util

X..... NLPPSU7 - 3746-900 Lne Prosr 7 Fast Pgm Stg Utl
X..... NLPPSU8 - 3746-900 Lne Prosr 8 Fast Pgm Stg Utl
X..... NLPPSU9 - 3746-900 Lne Prosr 9 Fast Pgm Stg Utl

5.2.17.3 Usage Considerations

This section identifies the special considerations or techniques related to using the SNTNLP file, followed by several retrieval examples.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &ddiit, where d is the database identifier, iiii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEK should not be used in MONTHS.
2. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7. For NPM, NETWRKID may be set to the value of the PLU Network Identifier (PLUNETID).
 - o TMOFFSET - Time offset applied to the data in the file. The user can associate a time offset with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. Time offset is assigned in the SNTOPS member of prefix.MICS.PARMS discussed in Chapter 7.

3. The following data elements lose significance once summarization has been performed. These data elements should only be referenced when the last observed value in a summarization interval is significant.

NPMTSFRU - Forward RU Send Time
NPMTSLOG - Time Record Logged to SMF
NPMTSEIS - Expected Interval Time

Retrieval Example

Produce a chart showing the CPU utilization for each network component for the month to date:

```
PROC CHART DATA=&PSNTX..SNTNLP01;  
  HBAR NETNAME / SUMVAR=NLPLPU1 DESCENDING;
```

5.2.18 Telnet Server Entry File (SNTNTS)

The Telnet Server Entry File (SNTNTS) contains data that quantifies TCP/IP Telnet session activity. The data is selected from CA NetSpy SMF record Subtype "I."

The SNTNTS file can also contain data from NetMaster Network Management for TCP/IP 11.0 or earlier.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.18.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	TCPIPHST	TCPRADDR	TCPLPORT	
	TCRPORT	YEAR	MONTH	DAY	HOUR	
	ENDTS					
DAYS	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	TCPIPHST	YEAR	MONTH	
	DAY	HOUR				
WEEKS	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	TCPIPHST	YEAR	WEEK	
	ZONE					
MONTHS	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	TCPIPHST	YEAR	MONTH	
	ZONE					
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=DEFault

option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-18. SNTNTS Timespan Granularity Chart

5.2.18.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XD...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	SNTACT1	- PRIMARY LOGICAL UNIT(PLU)
XDWM..E	SNTACT2	- SLUSAPU NETV/NPM1.3,SLUSA NPM1.2 OR NSPY

XDWM..E SNTACT3 - SLUPU IF NLDM OR NETSPY, SLU IF NPM
 XDWM..E SNTACT4 - NLDM PERFCLSS, NPM BLANK, NSPY/NAC SLU
 XDWM..E SNTACT5 - NOT-USED
 XDWM..E SYSID - System Identifier
 XDWM..E TCPIPHST - TCP/IP Host Name
 X.....E TCPLPORT - Local Port Number (Data Connection)
 X.....E TCPRADDR - Remote IP Address (Data Connection)
 X.....E TCPRPORT - Remote Port Number (Data Connection)
 XDWM..E WEEK - Week of Year
 XDWM..E YEAR - Year of Century
 XDWM..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
 X.....E DEVNUM - Device Number
 XDWM..E DURATION - Recording Interval Time
 XDWM..E ENDTS - End Time Stamp
 XDWM..E INTERVLS - Number of Recording Intervals
 XDWM..E MICSVER - CA MICS Version Number
 XDWM..E NTSBYTEI - Bytes Received From Client
 XDWM..E NTSBYTEO - Bytes Sent By the Server
 XDWM..E PRODUCT - Network Product (Source) Name
 XDWM..E STARTTS - Start Time Stamp
 X.....E TCPLADDR - Local IP Address (Data Connection)
 XD....E TCPSTQN - TCP/IP Address Space Name
 XDWM..E TMOFFSET - Time Offset

Retained Data Elements

X.....E NTSAPPL - Application Name
 XDWM..E NTSLTCHD - Last Touched
 X.....E NTSLU - Logical Unit Name
 X.....E NTSPCID - Procedure Correlation ID
 X.....E NTSPROTO - TCP/IP Protocol
 XDWM..E NTSRTT - Total of Round Trip Time
 XDWM..E NTSRTTV - Round Trip Time Variance
 XDWM..E NTSSLOWS - Slow Start
 XDWM..E NTSSTCIB - Smooth Time Change Since Beg. of Int.
 XDWM..E NTSSTIE - Smooth Time at Interval End
 XDWM..E NTSSTVIE - Smooth Time Variance at Interval End

Accumulated Data Elements

XDWM..E NTSACKI - Acknowledgements During the Interval
 XDWM..E NTSBYTER - Number of Retransmitted Bytes
 XDWM..E NTSDACKS - Duplicate ACKs

Maximum Data Elements

XDWM..E NTSCNGWN - Congestion Window
XDWM..E NTSMS - Maximum Send Segment Size
XDWM..E NTSMXSWN - Maximum Send Window
XDWM..E NTSMXUS - Max. TCBs With Unacknowledged Segmts.
XDWM..E NTSOSS - Optimal Segment Size

Derived Data Elements

XDWM..E NTSABTX - Average Bytes Transmitted
XDWM..E NTSTOTTX - Total Bytes Transmitted

5.2.18.3 Usage Considerations

This section identifies special considerations or techniques related to using the SNTNTS file. In addition, a retrieval example is provided to facilitate the use of this file.

CA MICS network session accounting/network gateway accounting supports the following versions of CA NetSpy, IBM Tivoli NetView Performance Monitor (NPM), and Network Control Program (NCP), or higher:

- o CA NetSpy Release 6.0 and later
- o NPM Version 2 and later
- o ACF/NCP Version 5 Release 2.1 and later

To prevent potentially serious problems with missing or duplicate data, do NOT use versions, releases, or revisions previous to those specified above.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEKS should not be used in MONTHS.
2. Avoid collecting redundant network session accounting and network gateway accounting data from either NPM or CA NetSpy. This is especially important if you input this data into the CA MICS Accounting and Chargeback product. The following SNTNAC elements can assist you in detecting redundant data:

NACCOLPT - NCP Collection Point
FUNCTION - Product Function
NACANPLU - Adjacent NETID PLU Side (NGA)
NACANSLU - Adjacent NETID SLU Side (NGA)
USESSIDC - Unique Session ID

An example of redundant data collection occurs when multiple gateway NCPs are traversed by a terminal to application session and each of these NCPs collects gateway accounting data for that session. In this case, the redundant data could be detected by the presence of multiple observations in the DETAIL timespan with identical Unique Session IDs, but different values for Adjacent NETID PLU Side or Adjacent NETID SLU Side. Refer to Section 8.1.3.3 of this guide, Redundant Information Issues, for further information on how to detect and eliminate duplicate network accounting data.

3. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID--Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7 of this guide.
 - o TMOFFSET--TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7 of this guide.

Retrieval Example

Chart prime shift TCP/IP Telnet Server activity for sysid PROD. Use yesterday's data.

```
DATA SELECTED (KEEP=SYSID DAY ZONE HOUR NTSBYTEI NTSBYTEO);  
SET &PSNTD..SNTNTS01;  
IF SYSID = 'PROD';  
IF 9 GE HOUR LE 17; /* SELECT PRIME SHIFT */  
  
PROC CHART DATA=SELECTED;
```

```
VBAR HOUR / SUMVAR=NTSBYTEI  
DISCRETE;  
TITLE 'DAYS SNTNTS01, PRIME SHIFT IN BYTE COUNT ';  
RUN;
```

5.2.19 Stack Entry File (SNTTCS)

The Stack Entry File (SNTTCS) contains data that quantifies TCP/IP address space activity. The data is selected from CA NetSpy SMF record subtype "J."

The SNTTCS file can also contain data from NetMaster Network Management for TCP/IP 11.0 or earlier.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.19.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	TCPSTQN	YEAR	MONTH	
	DAY	HOUR	ENDTS			
DAYS	NETWRKID	SYSID	TCPSTQN	YEAR	MONTH	
	DAY	HOUR				
WEEKS	NETWRKID	SYSID	TCPSTQN	YEAR	WEEK	
	ZONE					
MONTHS	NETWRKID	SYSID	TCPSTQN	YEAR	MONTH	
	ZONE					
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-19. SNTTCS Timespan Granularity Chart

5.2.19.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XD...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	SYSID	- System Identifier
XDWM..E	TCPSTQN	- TCP/IP Address Space Name

XDW...E WEEK - Week of Year
XDWM..E YEAR - Year of Century
XDWM..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
XDWM..E DURATION - Recording Interval Time
XDWM..E ENDTS - End Time Stamp
XDWM..E INTERVLS - Number of Recording Intervals
XDWM..E MICSVER - CA MICS Version Number
XDWM..E PRODUCT - Network Product (Source) Name
XDWM..E STARTTS - Start Time Stamp
XDWM.. TMOFFSET - Time Offset

Retained Data Elements

XDWM..E TCSIPLTS - TCP/IP IPL Date and Time

Accumulated Data Elements

XDWM..E TCSAOPEN - Active Opens
XDWM..E TCSFLSC - Number of Failed Connections
XDWM..E TCSPOPEN - Passive Opens
XDWM..E TCSRESET - Number of Resets
XDWM..E TCSRTXSG - Retransmitted Segments
XDWM..E TCSRXSEG - Received Segments
XDWM..E TCSTXSEG - Sent Segments
XDWM..E TCSWESEG - Segments With Errors

Minimum Data Elements

XDWM..E TCSMNRXT - Minimum Retransmission Time

Maximum Data Elements

XDWM..E TCSBUFR - Receive Buffer Size
XDWM..E TCSBUFS - Send Buffer Size
XDWM..E TCSCURCW - Current on Closed-Wait Connections
XDWM..E TCSLMSC - Limit on Number of Connections
XDWM..E TCSMXRXT - Maximum Retransmission Time
XDWM..E TCSMXSC - Maximum Number of Socket Connections

5.2.19.3 Usage Considerations

This section identifies special considerations or techniques related to using the SNTNTS file. In addition, a retrieval example is provided to facilitate the use of this file.

CA MICS network session accounting/network gateway accounting supports the following versions of CA NetSpy, IBM Tivoli NetView Performance Monitor (NPM), and Network Control Program (NCP), or higher:

- o CA NetSpy Release 6.0 and later
- o NPM Version 2 and later
- o ACF/NCP Version 5 Release 2.1 and later

To prevent potentially serious problems with missing or duplicate data, do NOT use versions, releases, or revisions previous to those specified above.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEKS should not be used in MONTHS.
2. Avoid collecting redundant network session accounting and network gateway accounting data from either NPM or CA NetSpy. This is especially important if you input this data into the CA MICS Accounting and Chargeback product. The following SNTNAC elements can assist you in detecting redundant data:

NACCOLPT - NCP Collection Point
FUNCTION - Product Function
NACANPLU - Adjacent NETID PLU Side (NGA)
NACANSLU - Adjacent NETID SLU Side (NGA)
USESSIDC - Unique Session ID

An example of redundant data collection occurs when multiple gateway NCPs are traversed by a terminal to application session and each of these NCPs collects gateway accounting data for that session. In this case, the redundant data can be detected by the presence of multiple observations in the DETAIL timespan with identical Unique Session IDs, but different values for Adjacent NETID PLU Side or Adjacent NETID SLU Side. Refer to Section 8.1.3.3 of this guide, Redundant Information Issues, for further information on how to detect and eliminate duplicate network accounting data.

3. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID--Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7 of this guide.
 - o TMOFFSET--TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7 of this guide.

Retrieval Example

Chart prime shift TCP/IP Telnet Server activity for sysid
PROD. Use yesterday's data.

```
DATA SELECTED (KEEP=SYSID DAY ZONE HOUR NTSBYTEI NTSBYTEO);  
SET &PSNTD..SNTNTS01;  
IF SYSID = 'PROD';  
IF 9 GE HOUR LE 17; /* SELECT PRIME SHIFT */  
  
PROC CHART DATA=SELECTED;  
    VBAR HOUR / SUMVAR=NTSBYTEI
```

```
DISCRETE;  
TITLE 'DAYS SNTNTS01, PRIME SHIFT IN BYTE COUNT ';  
RUN;
```

5.2.20 VTAM Buffer Pool Data File (SNTVBS)

The VTAM Buffer Data (SNTVBS) File contains data that quantifies VTAM buffer pool activity. The data is selected from CA NetSpy SMF record subtype "B" and/or Netview Performance Monitor (NPM) SMF record type 28 subtype X'D7'.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.20.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	SNTBUFID	VBSSPOOL	VBSUSR	
	YEAR	MONTH	DAY	HOURL	ENDTS	
DAYS	NETWRKID	SYSID	SNTBUFID	VBSSPOOL	VBSUSR	
	YEAR	MONTH	DAY	HOURL		
WEEKS	NETWRKID	SYSID	SNTBUFID	VBSSPOOL	VBSUSR	
	YEAR	WEEK	ZONE	HOURL		
MONTHS	NETWRKID	SYSID	SNTBUFID	VBSSPOOL	VBSUSR	
	YEAR	MONTH	ZONE			
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-20. SNTVBS Timespan Granularity Chart

5.2.20.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

X - DETAIL
 D - DAYS
 W - WEEKS
 M - MONTHS
 Y - YEARS
 T - TABLES AREA
 . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XDW...E	HOURL	- Hour of Day
XDWM..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	SNTBUFID	- Buffer Pool ID
XDWM..E	SYSID	- System Identifier

XDWM..E VBSSPOOL - Subpool Id
XDWM..E VBSUSR - Jobname or User ID
XDW...E WEEK - Week of Year
XDWM..E YEAR - Year of Century
XDWM..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
XDWM..E ENDTS - End Time Stamp
XDWM..E INTERVLS - Number of Recording Intervals
XDWM.. MICSVER - CA MICS Version Number
XDWM..E NETNAME - Resource Network Name
XDWM.. NPMTMAOT - Actual Observation Time
XDWM.. NPMTSEIS - Expected Interval Time
XDWM.. NPMTSFRU - Forward RU Send Time
XDWM..E PRODUCT - Network Product (Source) Name
XDWM..E PRODVRL - Product Version and Release
XDWM..E SAMPLES - Number of Samples
XDWM..E SNTSSCP - SSCP Name
XDWM..E STARTTS - Start Time Stamp
XDWM.. TMOFFSET - Time Offset

Retained Data Elements

XDWM..E VBSBFSZ - Bytes in Buffer (BUFSIZ)
XDWM..E VBSBFSZ2 - Bytes in Buffer (Adjusted BUFSIZ)
X.....E VBSEXPON - Dynamic Expansion On/Off
X.....E VBSSTYPE - Storage Type

Accumulated Data Elements

XDWM..E VBSACTEX - Total Active Extents
XDWM..E VBSAPDS - PLU to Diff. SA Traffic in IO Buffers
XDWM..E VBSAPSS - PLU to Same SA Traffic in IO Buffers
XDWM..E VBSAVLBF - Buffers Available in Extents
XDWM..E VBSBASE - Base Allocation in Buffers
XDWM..E VBSBASNO - Base Allocation Buffers - Static Area
XDWM..E VBSBASN2 - Base Allocation Bytes
XDWM..E VBSBFEXT - Buffers per Extents
XDWM..E VBSBFR - Buffers Used - CRPL Worst Offender
XDWM..E VBSCONTP - Contraction Point in Buffers
XDWM..E VBSEXPNP - Expansion Point in Buffers
XDWM..E VBSEXPNX - Buffers Over Expansion Point Count
XDWM..E VBSIRN - IRN Traffic in IO Buffers
XDWM..E VBSLCDS - SNA to Diff. SA Traffic in IO Buffers
XDWM..E VBSLND5 - nonSNA to Diff. SA Traffic in IO Buffers
XDWM..E VBSMISC - Miscellaneous Traffic in IO Buffers
XDWM..E VBSNCRPL - CRPL Buffers Used to Compute Worst Use

XDWM..E VBSNUMEX - Number of Expansions
XDWM..E VBSPAVL - Total Buffers Available
XDWM..E VBSPGEXT - Pages per Extents
XDWM..E VBSPTOT - Total Buffers Allocated
XDWM..E VBSPUSE - Total Buffers in Use
XDWM..E VBSRCCW - Read CCW in IO Buffers
XDWM..E VBSRESNO - Base Allocation Buffers - Residual Area
XDWM..E VBSSADS - SLU to Diff. SA Traffic in IO Buffers
XDWM..E VBSSLOWP - Slow Point in Buffers
XDWM..E VBSSLOWX - Buffers Over Slowdown Point Count
XDWM..E VBSSSCP - SSCP Traffic in IO Buffers
XDWM..E VBSTSCBS - TSCB Traffic in IO Buffers
XDWM..E VBSUNAL - Unallocated Traffic in IO Buffers
XDWM..E VBSVRPR - VR Pacing Resp. Traffic in IO Buffers
XDWM..E VBSXPNN0 - Expanded Buffers Count
XDWM..E VBSXPNN2 - Adjusted Expanded Buffers Count

Maximum Data Elements

XDWM..E VBSMXBFA - Max. Buffers Available
XDWM..E VBSMXBFR - Max. Buffers Used - D NET,BFRUSE
XDWM..E VBSMXBFU - Max. Buffers Used
XDWM..E VBSMXREQ - Max. Requesters Waiting
XDWM..E VBSMXTBA - Max. Buffers Allocated
XDWM..E VBSMXTBR - Max. Buffers Allocated - D NET,BFRUSE
XDWM..E VBSMXXPL - Max. Buffer Pool Size (XPANLIM)

Derived Data Elements

XDWM..E VBSPCU - Percent of CRPL use for This User

5.2.20.3 Usage Considerations

This section identifies the special considerations or techniques related to using the SNTVBS File. Additionally, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As the files' granularity increases in higher timespans, certain fields lose significance and should not be used in these cases:
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEK should not be used in MONTHS.
2. The following data elements are user-defined. The value in each is dependent on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - Time offset applied to the data in the file. The user can associate a time offset with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. Time offset is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

3. The following data elements lose significance once summarization has been performed. These data elements should only be referenced when the last observed value in a summarization interval is significant.

PRODVRRRL - Product Version and Release
TMOFFSET - Time Offset
VBSUSR - Jobname or Userid
VBSEXPON - Dynamic Expansion On/Off
VBSSTYPE - Storage Type

Retrieval Examples

1. Produce a report of the number of buffers allocated, used, and available, as well as the number of buffer expansions between the hours of 10 to 12 PM.

```
PROC PRINT DATA=&PSNTX..SNTVBS01;  
  WHERE HOUR GE 8 AND HOUR LE 12;  
  ID NETWRKID SYSID SNTBFID SNTSSCP VBSSPOOL;  
  VAR VBSBASE VBSPAVL VBSPUSE VBSNUMEX;
```

2. Produce a report showing the worst use of CRPL.

```
PROC PRINT DATA=&PSNTX..SNTVBS01;  
  ID NETWRKID SYSID SNTBFID VBSSSCP VBFUSR;  
  VAR VBSBFR VBSNCRPL VBSPCU;
```

5.2.21 VTAM CSM Data File (SNTVCS)

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.21.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	SNTSSCP	SNTCSMN	YEAR	
	MONTH	DAY	HOUR	ENDTS		
DAYS	NETWRKID	SYSID	SNTSSCP	SNTCSMN	YEAR	
	MONTH	DAY	HOUR			
WEEKS	NETWRKID	SYSID	SNTSSCP	SNTCSMN	YEAR	
	WEEK	ZONE	HOUR			
MONTHS	NETWRKID	SYSID	SNTSSCP	SNTCSMN	YEAR	
	MONTH	ZONE				
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-21. SNTVCS Timespan Granularity Chart

5.2.21.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

- XD...E DAY - Day of Month
- XDW...E HOUR - Hour of Day
- XDWM..E MONTH - Month of Year
- XDWM..E NETWKID - Network Identifier
- XDWM..E SNTCSMN - CSM Group Name

XDWM..E SNTSSCP - SSCP Name
 XDWM..E SYSID - System Identifier
 XDWM..E WEEK - Week of Year
 XDWM..E YEAR - Year of Century
 XDWM..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
 XDWM..E ENDTS - End Time Stamp
 XDWM..E INTERVLS - Number of Recording Intervals
 XDWM.. MICSVER - CA MICS Version Number
 XDWM..E NETNAME - Resource Network Name
 XDWM.. NPMTMAOT - Actual Observation Time
 XDWM.. NPMTSEIS - Expected Interval Time
 XDWM.. NPMTSFRU - Forward RU Send Time
 XDWM..E PRODUCT - Network Product (Source) Name
 XDWM..E PRODVRL - Product Version and Release
 XDWM..E SAMPLES - Number of Samples
 XDWM..E STARTTS - Start Time Stamp
 XDWM.. TMOFFSET - Time Offset

Retained Data Elements

XDWM..E VCSVDTYP - Data Type
 XDWM..E VCS04DSI - 4K Data Space CSM Buffer Size
 XDWM..E VCS04DSR - 4K Data Space CSM Buffer Source
 XDWM..E VCS04ESI - 4K ECSA CSM Buffer Size
 XDWM..E VCS04ESR - 4K ECSA CSM Buffer Source
 XDWM..E VCS16DSI - 16K Data Space CSM Buffer Size
 XDWM..E VCS16DSR - 16K Data Space CSM Buffer Source
 XDWM..E VCS16ESI - 16K ECSA CSM Buffer Size
 XDWM..E VCS16ESR - 16K ECSA CSM Buffer Source
 XDWM..E VCS32DSI - 32K Data Space CSM Buffer Size
 XDWM..E VCS32DSR - 32K Data Space CSM Buffer Source
 XDWM..E VCS32ESI - 32K ECSA CSM Buffer Size
 XDWM..E VCS32ESR - 32K ECSA CSM Buffer Source
 XDWM..E VCS60DSI - 60K Data Space CSM Buffer Size
 XDWM..E VCS60DSR - 60K Data Space CSM Buffer Source
 XDWM..E VCS60ESI - 60K ECSA CSM Buffer Size
 XDWM..E VCS60ESR - 60K ECSA CSM Buffer Source

Accumulated Data Elements

XDWM..E VCSCUREC - Current ECSA Storage Usage
 XDWM..E VCSCURFX - Current Fixed Storage Usage
 XDWM..E VCS04DAV - 4K Data Space Buffer Pool Available
 XDWM..E VCS04DUS - 4K Data Space Buffer Pool in Use
 XDWM..E VCS04EAV - 4K ECSA Buffer Pool Available

XDWM..E VCS04EUS - 4K ECSA Buffer Pool in Use
XDWM..E VCS16DAV - 16K Data Space Buffer Pool Available
XDWM..E VCS16DUS - 16K Data Space Buffer Pool in Use
XDWM..E VCS16EAV - 16K ECSA Buffer Pool Available
XDWM..E VCS16EUS - 16K ECSA Buffer Pool in Use
XDWM..E VCS32DAV - 32K Data Space Buffer Pool Available
XDWM..E VCS32DUS - 32K Data Space Buffer Pool in Use
XDWM..E VCS32EAV - 32K ECSA Buffer Pool Available
XDWM..E VCS32EUS - 32K ECSA Buffer Pool in Use
XDWM..E VCS60DAV - 64K Data Space Buffer Pool Available
XDWM..E VCS60DUS - 64K Data Space Buffer Pool in Use
XDWM..E VCS60EAV - 60K ECSA Buffer Pool Available
XDWM..E VCS60EUS - 60K ECSA Buffer Pool in Use

Maximum Data Elements

XDWM..E VCSMXESU - Max. ECSA Storage Usage
XDWM..E VCSMXFSU - Max. Fixed Storage Usage

5.2.21.3 Usage Considerations

This section identifies the special considerations or techniques related to using the SNTVCS File. Additionally, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As the files' granularity increases in higher timespans, certain fields lose significance and should not be used in these cases:
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEK should not be used in MONTHS.
2. The following data elements are user-defined. The value in each is dependent on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - Time offset applied to the data in the file. The user can associate a time offset with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. Time offset is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

3. The following data elements lose significance once summarization has been performed. These data elements should only be referenced when the last observed value in a summarization interval is significant.

PRODVRRRL - Product Version and Release
TMOFFSET - Time Offset
VCSVDTYP - Data Type
VCS04DSR - Dynamic Expansion On/Off
VCS16DSR - Storage Type
VCS04DSR - 4K Data Space CSM Buffer Source
VCS16DSR - 16K Data Space CSM Buffer Source
VCS32DSR - 32K Data Space CSM Buffer Source
VCS60DSR - 60K Data Space CSM Buffer Source
VCS04ESR - 4K ECSA CSM Buffer Source
VCS16ESR - 16K ECSA CSM Buffer Source
VCS32ESR - 32K ECSA CSM Buffer Source
VCS60ESR - 60K ECSA CSM Buffer Source
VCS04DSI - 4K Data Space CSM Buffer Size
VCS16DSI - 16K Data Space CSM Buffer Size
VCS32DSI - 32K Data Space CSM Buffer Size
VCS60DSI - 60K Data Space CSM Buffer Size
VCS04ESI - 4K ECSA CSM Buffer Size
VCS16ESI - 16K ECSA CSM Buffer Size
VCS32ESI - 32K ECSA CSM Buffer Size
VCS60ESI - 60K ECSA CSM Buffer Size

Retrieval Examples

1. Produce a report for CSM storage use.

```
PROC PRINT DATA=&PSNTX..SNTVCS01;  
  WHERE VCSVDTYP = 'STORAGE';  
  ID NETWRKID SYSID SNTSSCP SNTCSM;  
  VAR VCSMXFSU VCSMXESU VCSCURFX VCSCUREC;
```


5.2.22 VTAM Global Data File (SNTVGB)

The VTAM Global data (SNTVGB) File contains data that quantifies VTAM global information used for VTAM startup options, VTAM CPU usage, VTAM pages in and out, storage allocated, etc. The data is selected from Netview Performance Monitor (NPM) SMF record type 28 subtype X'D6'.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.2.22.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	SNTSSCP	YEAR	MONTH	
	DAY	HOUR	ENDTS			
DAYS	NETWRKID	SYSID	SNTSSCP	YEAR	MONTH	
	DAY	HOUR				
WEEKS	NETWRKID	SYSID	SNTSSCP	YEAR	WEEK	
	ZONE	HOUR				
MONTHS	NETWRKID	SYSID	SNTSSCP	YEAR	MONTH	
	ZONE					
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-22. SNTVGB Timespan Granularity Chart

5.2.22.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XDW...E	HOURL	- Hour of Day
XDWM..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	SNTSSCP	- SSCP Name
XDWM..E	SYSID	- System Identifier

XDW...E WEEK - Week of Year
 XDWM..E YEAR - Year of Century
 XDWM..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
 XDWM..E ENDTS - End Time Stamp
 XDWM..E INTERVLS - Number of Recording Intervals
 XDWM.. MICSVER - CA MICS Version Number
 XDWM..E NETNAME - Resource Network Name
 XDWM.. NPMTMAOT - Actual Observation Time
 XDWM.. NPMTSEIS - Expected Interval Time
 XDWM.. NPMTSFRU - Forward RU Send Time
 XDWM..E PRODUCT - Network Product (Source) Name
 XDWM..E PRODVRL - Product Version and Release
 XDWM..E SAMPLES - Number of Samples
 XDWM..E STARTTS - Start Time Stamp
 XDWM.. TMOFFSET - Time Offset

Retained Data Elements

XDWM..E VGBCSASZ - System CSA24 Size in Bytes - Below
 XDWM..E VGBCSAS - System CSA Size in Bytes - Above
 XDWM..E VGBTCAS - System CSA Size In Bytes - Total
 XDWM..E VGBTNSTA - VTAM Tuning Statistics Type

Accumulated Data Elements

XDWM..E VGBASCBS - System Active Jobnames or User IDs
 XDWM..E VGBCACSA - CSA Allocated
 XDWM..E VGBCAC24 - CSA24 Allocated
 XDWM..E VGBCNDLR - Dump/Load/Restore Requests
 XDWM..E VGBCRPSA - Private Storage Allocated
 XDWM..E VGBESCT - VTAM Extended Frame Count
 XDWM..E VGBFMCT - VTAM Frame Count
 XDWM..E VGBHCSAC - CSA Highwater Mark
 XDWM..E VGBHCSAS - CSA Highwater Mark - D NET,BFRUSE
 XDWM..E VGBHC24C - CSA24 Highwater Mark
 XDWM..E VGBHC24S - CSA24 Highwater Mark - D NET,BFRUSE
 XDWM..E VGBIACTC - VTAM Active CTC Devices
 XDWM..E VGBIALOC - VTAM Active non-SNA Devices
 XDWM..E VGBIAMPR - VTAM Active MPC Read Devices
 XDWM..E VGBIAMPW - VTAM Active MPC Write Devices
 XDWM..E VGBIANCP - VTAM Active NCP Devices
 XDWM..E VGBIAOTH - VTAM Active Other Devices
 XDWM..E VGBIASNA - VTAM Active SNA Devices
 XDWM..E VGBIATOT - VTAM Active Total Devices
 XDWM..E VGBITCTC - VTAM SIOs to CTC Devices

XDWL..E VGBITDS - VTAM SIOs to DASD
XDWL..E VGBITLOC - VTAM SIOs to Local non-SNA Devices
XDWL..E VGBITMPR - VTAM SIOs to MPC Read Devices
XDWL..E VGBITMPW - VTAM SIOs to MPC Write Devices
XDWL..E VGBITNCP - VTAM SIOs to NCPs
XDWL..E VGBITOTH - VTAM SIOs to Other Devices
XDWL..E VGBITSNA - VTAM SIOs to Local SNA Devices
XDWL..E VGBITTOT - VTAM SIOs to All Devices
XDWL..E VGBTCAPI - VTAM Total Common Page-ins
XDWL..E VGBTEJST - VTAM Total TCB Time
XDWL..E VGBTLPAI - VTAM Total LPA Page-ins
XDWL..E VGBTPAGE - VTAM Total Page-ins
XDWL..E VGBTPIN - VTAM Total Private Page-ins
XDWL..E VGBTSRBT - VTAM Total SRB Time
XDWL..E VGBTTIME - VTAM Total CPU Time
XDWL..E VGBTWSS - VTAM Working Set Size Count - Target
XDWL..E VGBWSS - VTAM Working Set Size Count

Maximum Data Elements

XDWL..E VGBMEDLR - Max. Dump/Load/Restore Requests Ever
XDWL..E VGBMHCSC - Max. CSA Highwater Mark
XDWL..E VGBMHCSS - Max. CSA Highwater Mark - D NET,BFRUSE
XDWL..E VGBMHC24 - Max. CSA24 Highwater Mark
XDWL..E VGBMHS24 - Max. CSA24 Highwater Mark - D NET,BFRUSE
XDWL..E VGBMXCSA - Max. CSA Allowed (CSALIMIT Spec.)
XDWL..E VGBMXCSU - Max. CSA Used - D NET,BFRUSE
XDWL..E VGBMXC24 - Max. CSA24 Allowed (CSA24 Spec.)
XDWL..E VGBMXDLR - Max. Dump/Load/Restore Requests
XDWL..E VGBMXPSA - Max. Private Storage Allocated
XDWL..E VGBMXU24 - Max. CSA24 Used - D NET,BFRUSE

5.2.22.3 Usage Considerations

This section identifies the special considerations or techniques related to using the SNTVGB File. Additionally, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As the file's granularity increases in higher timespans certain fields lose significance and should not be used in these cases:
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEK should not be used in MONTHS.
2. The following data elements are user-defined. The value in each is dependent on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - Time offset applied to the data in the file. The user can associate a time offset with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. Time offset is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

3. The following data elements lose significance once summarization has been performed. These data elements should only be referenced when the last observed value in a summarization interval is significant.

PRODVRRRL - Product Version and Release
TMOFFSET - Time Offset
VGBTNSTA - VTAM Tuning Statistics Type
VGBCSASZ - System CSA24 Size in Bytes - Below
VGBECSAS - System CSA Size in Bytes - Above
VGBTCAS - System CSA Size In Bytes - Total

Retrieval Examples

1. Produce a report on the VTAM CPU utilization.

```
PROC PRINT DATA=&PSNTX..SNTVGB01;  
  ID NETWRKID SYSID SNTSSCP;  
  VAR VGBTTIME VGBTEJST VGBTSRBT;
```

5.3 NVS Information Area

The NVS Information Area captures information about NetView sessions in the files described in this chapter:

- 1 - NLDM System (PLU) Activity File (NVSLSY)
- 2 - NLDM Session Accounting File (NVSNSA)
- 3 - NLDM Session Connectivity File (NVSNSC)
- 4 - NLDM Link Activity File (NVSNULL)
- 5 - NLDM Route File (NVS RTE)
- 6 - NLDM Response Time File (NVSRTM)
- 7 - NLDM VTAM Bind Failure File (NVS VBF)

5.3.1 NLDM System (PLU) Activity File (NVSLSY)

The NLDM System (PLU) Activity File (NVSLSY) quantifies response time and network traffic statistics by primary logical unit (usually an application, such as TSO or CICSTEST) and user-defined performance class.

This file is derived from the NLDM Session Connectivity (NVSNSC), NLDM Response Time (NVSRTM), and NLDM Session Accounting (NVSNSA) files.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.3.1.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	N/A					
DAYS	NETWRKID	SYSID	PLU	PERFCLSS	YEAR	
	MONTH	DAY	HOUR			
WEEKS	NETWRKID	SYSID	PLU	PERFCLSS	YEAR	
	WEEK	ZONE	HOUR			
MONTHS	NETWRKID	SYSID	PLU	PERFCLSS	YEAR	
	MONTH	ZONE				
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=DEFAult option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-17. NVLSY Timespan Granularity Chart

5.3.1.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

.D...E	DAY	- Day of Month
.DW...E	HOURL	- Hour of Day
.D.M..E	MONTH	- Month of Year
.DWM..E	NETWRKID	- Network Identifier
.DWM..E	PERFCLSS	- Performance Class (NLDM)
.DWM..E	PLU	- Primary Logical Unit

.DWM..E SYSID - System Identifier
 .DW...E WEEK - Week of Year
 .DWM..E YEAR - Year of Century
 .DWM..E ZONE - Time Zone

Common Data Elements

.D....E DAYNAME - Name of Day of Week
 .DWM.. DURATION - Recording Interval Time
 .DWM..E ENDTS - End Time Stamp
 .DWM.. MICSVER - CA MICS Version Number
 .DWM.. NLDMVRRL - NLDM Version and Release Id
 .DWM..E NLDRVAL1 - NLDM Response Distribution Limits 1
 .DWM..E NLDRVAL2 - NLDM Response Distribution Limits 2
 .DWM..E NLDRVAL3 - NLDM Response Distribution Limits 3
 .DWM..E NLDRVAL4 - NLDM Response Distribution Limits 4
 .D.... NVSPRNM - Primary Endpoint CP Name
 .D.... NVSPRNT - Primary Endpoint CP Network ID
 .D.... NVSSCNM - Secondary Endpoint CP Name
 .D.... NVSSCNT - Secondary Endpoint CP Network ID
 .DWM.. PLDOMAIN - PLU Domain Name
 .DWM.. PLUSAPU - PLU Subarea Physical Unit
 .DWM.. PRODUCT - Network Product (Source) Name
 .DWM..E SAMPLES - Number of Samples
 SESTYPE - Session Type
 .DWM.. SLDOMAIN - SLU Domain Name
 SLU - Secondary Logical Unit
 SLULINK - SLU Link
 SLUPU - SLU Physical Unit
 .DWM.. SLUSAPU - SLU Subarea Physical Unit
 .DWM..E STARTTS - Start Time Stamp
 .DWM.. TMOFFSET - Time Offset

Retained Data Elements

.DWM.. LSYCNTR - Objective Counter Number
 .D.... LSYCOS - Class of Service
 .D.... LSYEXRTE - Explicit Route Number
 .DWM.. LSYPCOBJ - Objective Percentage
 .DWM.. LSYRDEF - Response Definition
 .DWM.. LSYROBTM - Objective Response Time
 .D.... LSYRVER - Reverse Explicit Route Number
 .D.... LSYTRPTY - Transmission Priority
 .D.... LSYVRTE - Virtual Route Number
 .D.... LSYXNET - Cross-network Session (Y or N)

Accumulated Data Elements

.DWM.. LSYNRCBR - Number Control Bytes Received

.DWM.. LSYNRCBS - Number Control Bytes Sent
.DWM..E LSYNRCPR - Number Control PIUs Received
.DWM..E LSYNRCPS - Number Control PIUs Sent
.DWM..E LSYNRROM - Number of Times Resp Obj Met
.DWM.. LSYNRTBR - Number Text Bytes Received
.DWM..E LSYNRTBS - Number Text Bytes Sent
.DWM..E LSYNRTPR - Number Text PIUs Received
.DWM..E LSYNRTPS - Number Text PIUs Sent
.DWM..E LSYRDST1 - Response Dist Count 1 (Boundary A)
.DWM..E LSYRDST2 - Response Dist Count 2 (Boundary B)
.DWM..E LSYRDST3 - Response Dist Count 3 (Boundary C)
.DWM..E LSYRDST4 - Response Dist Count 4 (Boundary D)
.DWM..E LSYRDST5 - Response Dist Count 5 (Above A,B,C,D)
.DWM..E LSYTRES - Response Event Count
.DWM..E LSYTRSTM - Total Response Time

Derived Data Elements

.DW... LSYAVCBR - Average Bytes per PIU Recvd (Control)
.DW... LSYAVCBS - Average Bytes per PIU Sent (Control)
.DW... LSYAVTBR - Average Bytes per PIU Recvd (Text)
.DW...E LSYAVTBS - Average Bytes per PIU Sent (Text)
.DWM..E LSYAVTTM - Average Total Response Time
.DWM..E LSYPCOBM - Pct of Times Response Obj Met
.DWM..E LSYPCTR1 - Cum. Pct All Resp Within Limit 1
.DWM..E LSYPCTR2 - Cum. Pct All Resp Within Limit 2
.DWM..E LSYPCTR3 - Cum. Pct All Resp Within Limit 3
.DWM..E LSYPCTR4 - Cum. Pct All Resp Within Limit 4

5.3.1.3 Usage Considerations

This section identifies special considerations or techniques related to using the NVSLSY File. In addition, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. The NLDM System Activity (NVSLSY) File and the NLDM Link Activity (NVSNULL) File combine data from two separate collection functions within the same monitor. That is, these files either combine two collection functions within IBM Tivoli NetView Performance Monitor or two collection functions within CA NetMaster.

From NetView, this file combines data from the RTM and A&A data collection functions. If both functions are turned on in NetView, then RTM and A&A data is automatically forwarded to NetView and combined in a session termination record, even if the data is not actively solicited via COLLECT and RECORD commands.

From CA NetMaster, this file combines data from the Network Tracking System component (NTS) RTM collection function and the accounting data collection function.

You must ensure that these two data collection functions are synchronized or the data from the two functions in each file represent information from different time periods.

To synchronize NetView Response Time Monitor (RTM) data and NetView accounting and availability (A&A) data collection, execute the NetView COLLECT and NetView RECORD commands simultaneously at regular intervals throughout the day via NetView/NCCF CLISTs. (See Chapter 6 for a

discussion of the sample CLISTs shipped with NetView for the COLLECT and RECORD commands.)

- o The NetView COLLECT command produces the SMF type 39 interval record that contains RTM data.
- o The NetView RECORD command produces the the SMF type 39 interval record that contains A&A data.

On NetView hosts that control large network domains, you may not be able to synchronize the collection of RTM and A&A data on a domain-wide basis. For example, if a NetView domain contains 2,000 or more remote 3274/3174 cluster controllers with the RTM feature, several minutes may elapse from the time the NetView COLLECT command executes until the time NetView receives RTM data from all of the remote controllers. A similar delay does not occur when A&A data is received because it is extracted internally from VTAM.

A possible solution is to synchronize the collection of A&A and RTM data for a subset of network resources within a NetView domain. For example, if you want to use the data as it is organized in the NLDM Link Activity (NVSNULL) File, synchronize execution of the NetView COLLECT and RECORD commands for all the resources attached to a given NCP or link. If the arrangement of data in the NLDM System Activity (NVSLSY) File is more useful to your data center, synchronize collection of the A&A and RTM data by primary logical unit (PLU).

For information on how to synchronize RTM data collection and accounting data collection from the Network Tracking System (NTS) and the Network Error Warning System (NEWS), two components of CA NetMaster Network Management for SNA, see the CA NetMaster NM for SNA Getting Started guide, Administration Guide, and other documentation.

2. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEKS should not be used in MONTHS.

3. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one- to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.
4. The following data elements lose significance once summarization has been performed. These data elements should only be referenced when the last observed value in a summarization interval is significant.

NLDMVRR - NLDM Version and Release ID
NLDRVAL1 - NLDM Response Distribution Limits 1
NLDRVAL2 - NLDM Response Distribution Limits 2
NLDRVAL3 - NLDM Response Distribution Limits 3
NLDRVAL4 - NLDM Response Distribution Limits 4
PLDOMAIN - PLU Domain Name
PLUSAPU - PLU Subarea Physical Unit
SLDOMAIN - SLU Domain Name
SLU - Secondary Logical Unit
SLULINK - SLU Link
SLUPU - SLU Physical Unit
SLUSAPU - SLU Subarea Physical Unit
TMOFFSET - TIME OFFSET
LSYCNTR - Objective Counter Number
LSYCOS - Class of Service
LSYXRTE - Explicit Route Number
LSYPCOBJ - Objective Percentage
LSYRDEF - Response Definition
LSYROBTM - Objective Response Time
LSYRVER - Reverse Explicit Route Number
SESTYPE - Session Type
LSYTRPTY - Transmission Priority
LSYVRTE - Virtual Route Number
LSYXNET - Cross-network Session

5. For TSO sessions, both NetView and CA NetMaster record multiple values for the primary logical unit (PLU) for sessions with a single TSO system. These duplicate values are carried over into the CA MICS data for TSO sessions in the element PLU. This can greatly increase the size of the NVSLSY File because PLU is a sequence/summary element. This problem can be circumvented by the user-coded routine in prefix.MICS.PARMS(SNTPLURT), which sets the multiple values for PLU to a single value for each TSO system. Refer to Section 7.10 for information about SNTPLURT.

Retrieval Example

Chart prime shift response time for primary logical units; TS008, TS009, IMSPROD, and DBDCCICS. Use yesterday's data.

```
DATA SELECTED (RENAME=(PLU=APPL LSYAVTTM=RESPONSE));
SET &PNVSD..NVSLSY01;
IF PLU='TS008' OR PLU='TS009' OR PLU='DBDCCICS' OR
   PLU='IMSPROD';
IF 9 GE HOUR LE 17; /* SELECT PRIME SHIFT */

PROC CHART DATA=SELECTED;
  VBAR HOUR / SUMVAR=RESPONSE
  GROUP=APPL
  DISCRETE;
TITLE 'DAYS NVSLSY01, PRIME SHIFT AVG RESPONSE TIME ';
RUN;
```

5.3.2 NLDM Session Accounting File (NVSNSA)

The NLDM Session Accounting File (NVSNSA) quantifies network traffic and session connect time by user-defined account code. You can use this data to determine the use of or to charge for network resources such as terminals and/or cluster controllers.

This file is derived from the NetView Session Monitor/NLDM External Log Record or the CA NetMaster NTS SMF Record.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.3.2.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	SESTYPE	YEAR	MONTH	
	DAY	HOUR	ENDTS			
DAYS	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	SESTYPE	YEAR	MONTH	
	DAY	HOUR				
WEEKS	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	SESTYPE	YEAR	WEEK	
	ZONE	HOUR				
MONTHS	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	SESTYPE	YEAR	MONTH	
	ZONE					
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not

is controlled by the complex definition of the
DERIVED option.

Figure 5-18. NVSNSA Timespan Granularity Chart

5.3.2.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

X - DETAIL
 D - DAYS
 W - WEEKS
 M - MONTHS
 Y - YEARS
 T - TABLES AREA
 . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XDW...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	SESTYPE	- Session Type
XDWM..E	SNTACT1	- PRIMARY LOGICAL UNIT(PLU)
XDWM..E	SNTACT2	- SLUSAPU NETV/NPM1.3,SLUSA NPM1.2 OR NSPY

XDW..E SNTACT3 - SLUPU IF NLDM OR NETSPY, SLU IF NPM
XDW..E SNTACT4 - NLDM PERFCLSS, NPM BLANK, NSPY/NAC SLU
XDW..E SNTACT5 - NOT-USED
XDW..E SYSID - System Identifier
XDW...E WEEK - Week of Year
XDW..E YEAR - Year of Century
XDW..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
XDW.. DURATION - Recording Interval Time
XDW..E ENDTS - End Time Stamp
XDW.. MICSVER - CA MICS Version Number
X....E NETGROUP - Network Service Group
XDW.. NLDMVRRL - NLDM Version and Release Id
X.... NVSPRNM - Primary Endpoint CP Name
X.... NVSPRNT - Primary Endpoint CP Network ID
X.... NVSSCNM - Secondary Endpoint CP Name
X.... NVSSCNT - Secondary Endpoint CP Network ID
XD.... PERFCLSS - Performance Class (NLDM)
XD.... PLU - Primary Logical Unit
XDW.. PRODUCT - Network Product (Source) Name
XDW.. SAMPLES - Number of Samples
XD....E SLU - Secondary Logical Unit
XD.... SLULINK - SLU Link
XDW..E STARTTS - Start Time Stamp
XDW.. TMOFFSET - Time Offset
X.... USESSIDC - Unique Session ID (Character)

Retained Data Elements

XD.... NSAXDMN - Cross-domain Session (Y or N)

Accumulated Data Elements

XDW..E NSACONTM - Connect Time
XDW.. NSACOST - Billable Cost
XDW..E NSANRCBR - Number Control Bytes Received
XDW..E NSANRCBS - Number Control Bytes Sent
XDW..E NSANRCPR - Number Control PIUs Received
XDW..E NSANRCPS - Number Control PIUs Sent
XDW..E NSANRTBR - Number Text Bytes Received
XDW..E NSANRTBS - Number Text Bytes Sent
XDW..E NSANRTPR - Number Text PIUs Received
XDW..E NSANRTPS - Number Text PIUs Sent

Derived Data Elements

XDWM.. NSAAVCBR - Average Bytes per PIU Recvd (Cntl)
XDWM.. NSAAVCBS - Average Bytes per PIU Sent (Cntl)
XDWM.. NSAAVTBR - Average Bytes per PIU Recvd (Text)
XDWM.. NSAAVTBS - Average Bytes per PIU Sent (Text)
XDWM..E NSANRTBY - Total Number of Bytes Transmitted
XDWM.. NSANRTPI - Total Number of PIUs Transmitted

5.3.2.3 Usage Considerations

This section identifies special considerations or techniques related to using the NVSNSA File. In addition, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEKS should not be used in MONTHS.
2. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.
3. The following data elements lose significance once

summarization has been performed, unless they are used in the summarization sequence as a result of being included in one of the accounting fields (i.e., SNTACT1, SNTACT2, etc.).

NLDMVRRL - NLDM Version and Release ID
 PLU - Primary Logical Unit
 SLU - Secondary Logical Unit
 SLULINK - SLU Link
 NSAXDMN - Cross-domain Session (Y or N)

4. For TSO sessions, both NetView and CA NetMaster record multiple values for the primary logical unit (PLU) for sessions with a single TSO system. These duplicate values are carried over into the CA MICS data for TSO sessions in the element PLU. This can greatly increase the size of the file if PLU is chosen as one of the account codes. You can circumvent this problem with the user-coded routine in prefix.MICS.PARMS(SNTPLURT), which sets the multiple values for PLU to a single value for each TSO system. Refer to Section 7.10 for information about SNTPLURT.

Retrieval Example

Report connect time last week for the applications TS008, TS009, DBDCCICS, and IMSPROD by zone.

```
DATA SELECTED (RENAME=(PLU=APPL NSACONTM=CONNECT));
SET &PNVSW..NVSNSA01;
IF PLU='TS008' OR PLU='TS009' OR PLU='DBDCCICS' OR
   PLU='IMSPROD';
IF DAYNAME NE 'SAT' OR DAYNAME NE 'SUN';
ZONENAM=PUT(ZONE,$ZONENM.);

PROC PRINT DATA=SELECTED; VAR DAYNAME CONNECT;
BY NETWRKID SYSID ZONENAM;
TITLE 'WEEKS NVSNSA01, MON-FRI APPL CONNECT TIME ';
```

5.3.3 NLDM Session Connectivity File (NVSNSC)

The NLDM Session Connectivity File (NVSNSC) contains all of the available configuration information for each session by user-defined account code. One observation is maintained for each unique SNA session for which data was recorded during the collection time period (usually one day).

This file is derived from the NetView Session Monitor/NLDM External Log Record or the CA NetMaster NTS SMF Record.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.3.3.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	SESTYPE	YEAR	MONTH	
	DAY	HOUR	ENDTS			
DAYS	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	SESTYPE	YEAR	MONTH	
	DAY	HOUR				
WEEKS	N/A					
MONTHS	N/A					
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-19. NVSNSC Timespan Granularity Chart

5.3.3.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

X - DETAIL
D - DAYS
W - WEEKS
M - MONTHS
Y - YEARS
T - TABLES AREA
. - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD....E	DAY	- Day of Month
XD....E	HOURL	- Hour of Day
XD....E	MONTH	- Month of Year
XD....E	NETWRKID	- Network Identifier
XD....E	SESTYPE	- Session Type
XD....E	SNTACT1	- PRIMARY LOGICAL UNIT(PLU)

XD....E SNTACT2 - SLUSAPU NETV/NPM1.3,SLUSA NPM1.2 OR NSPY
 XD....E SNTACT3 - SLUPU IF NLDM OR NETSPY, SLU IF NPM
 XD....E SNTACT4 - NLDM PERFCLSS, NPM BLANK, NSPY/NAC SLU
 XD....E SNTACT5 - NOT-USED
 XD....E SYSID - System Identifier
 XD....E WEEK - Week of Year
 XD....E YEAR - Year of Century
 XD....E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
 XD....E ENDTS - End Time Stamp
 XD.... INTERVLS - Number of Recording Intervals
 XD.... MICSVER - CA MICS Version Number
 X.... NETGROUP - Network Service Group
 XD.... NLDMMVRL - NLDM Version and Release Id
 X.... NVSPRNM - Primary Endpoint CP Name
 X.... NVSPRNT - Primary Endpoint CP Network ID
 X.... NVSSCNM - Secondary Endpoint CP Name
 X.... NVSSCNT - Secondary Endpoint CP Network ID
 X....E ORGSYSID - Originating System Identification
 XD.... PERFCLSS - Performance Class (NLDM)
 XD.... PLDOMAIN - PLU Domain Name
 XD....E PLU - Primary Logical Unit
 XD.... PLUPU - Primary Logical Unit Physical Unit
 XD....E PLUSAPU - PLU Subarea Physical Unit
 XD.... PRIMLINK - Primary Link (NLDM)
 XD.... PRODUCT - Network Product (Source) Name
 X.... SLDOMAIN - SLU Domain Name
 X....E SLU - Secondary Logical Unit
 XD....E SLULINK - SLU Link
 XD....E SLUPU - SLU Physical Unit
 XD....E SLUSAPU - SLU Subarea Physical Unit
 XD....E STARTTS - Start Time Stamp
 XD.... TMOFFSET - Time Offset
 X....E USESSIDC - Unique Session ID (Character)

Retained Data Elements

X.... NSCCOS - Class of Service
 X....E NSCDATAM - NetView Data Mask
 X.... NSCEXRTE - Explicit Route Number
 X.... NSCLDEV - Locally Attached Device (Y or N)
 X.... NSCRVER - Reverse Explicit Route Number
 X....E NSCSEMSK - Session Mask
 X.... NSCTRPTY - Transmission Priority
 X....E NSCVR RTE - Virtual Route Number
 XD.... NSCXDMN - Cross-domain Session (Y or N)

XD.... NSCXNET - Cross-network Session

Accumulated Data Elements

XD....E NSCCONTM - Connect Time

XD.... NSCCOST - Billable Cost

XD.... NSCNMSES - Number of Sessions

XD....E NSCNRTCH - Total Characters Transmitted

5.3.3.3 Usage Considerations

This section identifies special considerations or techniques related to using the NVSNSC File. In addition, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEKS should not be used in MONTHS.
2. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

3. The following data elements lose significance once summarization has been performed, unless they are used in the summarization sequence as a result of being included in one of the accounting fields (i.e., SNTACT1, SNTACT2, etc.).

NLDMVRR - NLDM Version and Release ID
PLDOMAIN - PLU Domain Name
PLU - Primary Logical Unit
PLUPU - Primary Logical Unit Physical Unit
PLUSAPU - PLU Subarea Physical Unit
PRIMLINK - Primary Link (NLDM)
SESTYPE - Session Type
SLDOMAIN - SLU Domain Name
SLU - Secondary Logical Unit
SLULINK - SLU Link
SLUPU - SLU Physical Unit
SLUSAPU - SLU Subarea Physical Unit
TMOFFSET - TIME OFFSET
NSCCOS - Class of Service
NSCEXRTE - Explicit Route Number
NSCRVER - Reverse Explicit Route Number
NSCTRPTY - Transmission Priority
NSCVRTE - Virtual Route Number
NSCXDMN - Cross-domain Session (Y or N)
NSCXNET - Cross-network Session

4. The following are two special problems regarding TSO sessions and the element PLU. These two problems are as follows:
- o Both NetView and CA NetMaster record two sessions for every TSO user session. This number is carried in the CA MICS element Number of Sessions (NSCNMSES).
 - o The PLU element carries multiple values for sessions with a single TSO system. This can greatly increase the size of the file if PLU is chosen as one of the account codes.

This problem can be circumvented by the user-coded routine in prefix.MICS.PARMS(SNTPLURT), which sets the multiple values for PLU to a single value for each TSO system. Refer to Section 7.10 for information about SNTPLURT.

Retrieval Example

Report the prime shift application statistics for yesterday.

```
/* SET THE BY AND BREAK SUMMARY MACROS */
%LET BY = NETWRKID SYSID PLU;
%LET BREAK = PLU;

PROC SORT DATA=&PNVSD..NVSNSC01 OUT=SORTED;BY &BY;
RUN;

DATA SUMMED (RENAME=(PLU=APPL NSCCONTM=CONNECT
                     NSCNMSES=SESSIONS NSCNRTCH=TRAFFIC));
SET SORTED;
%NSCSUM;          /* SUM THE DATA */
RUN;

DATA SUMMED;
SET SUMMED;
IF 9 GT HOUR LE 17; /* SELECT PRIME SHIFT */

PROC PRINT;VAR APPL SESSIONS CONNECT TRAFFIC;
TITLE 'DAYS NVSNSC01, PRIME SHIFTE APPL STATISTICS';
RUN;
```

5.3.4 NLDM Link Activity File (NVSNLL)

The NLDM Link Activity File (NVSNLL) quantifies response time and input/output character traffic so you can correlate network service to traffic for sessions across specific links that are associated with user-defined performance classes.

This file is derived from the NLDM Session Accounting (NVSNSA), NLDM Response Time (NVSRTM), and NLDM Session Connectivity (NVSNSC) files.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.3.4.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

+-----+-----+-----+-----+-----+-----+-----+						
Timespan	Level of Data Granularity					
+-----+-----+-----+-----+-----+-----+-----+						
DETAIL	N/A					
DAYS	NETWRKID	SYSID	SLUSAPU	SLULINK	PERFCLSS	
	YEAR	MONTH	DAY	HOURL		
WEEKS	NETWRKID	SYSID	SLUSAPU	SLULINK	PERFCLSS	
	YEAR	WEEK	ZONE	HOURL		
MONTHS	NETWRKID	SYSID	SLUSAPU	SLULINK	PERFCLSS	
	YEAR	MONTH	ZONE			
YEARS	N/A					
+-----+-----+-----+-----+-----+-----+-----+						
TABLES	N/A					
+-----+-----+-----+-----+-----+-----+-----+						

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-20. NVSNLL Timespan Granularity Chart

5.3.4.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

.D...E	DAY	- Day of Month
.DW...E	HOURL	- Hour of Day
.D.M..E	MONTH	- Month of Year
.DWM..E	NETWRKID	- Network Identifier
.DWM..E	PERFCLSS	- Performance Class (NLDM)
.DWM..E	SLULINK	- SLU Link
.DWM..E	SLUSAPU	- SLU Subarea Physical Unit

.DWM..E SYSID - System Identifier
 .DW...E WEEK - Week of Year
 .DWM..E YEAR - Year of Century
 .DWM..E ZONE - Time Zone

Common Data Elements

.D....E DAYNAME - Name of Day of Week
 .DWM.. DURATION - Recording Interval Time
 .DWM..E ENDTs - End Time Stamp
 .DWM.. LNKTpCID - Network Link TP Circuit Id
 .DWM.. MICSVER - CA MICS Version Number
 .DWM.. NLDmVRRL - NLDm Version and Release Id
 .DWM..E NLDmVAL1 - NLDm Response Distribution Limits 1
 .DWM..E NLDmVAL2 - NLDm Response Distribution Limits 2
 .DWM..E NLDmVAL3 - NLDm Response Distribution Limits 3
 .DWM..E NLDmVAL4 - NLDm Response Distribution Limits 4
 .D.... NVSPRNM - Primary Endpoint CP Name
 .D.... NVSPRNT - Primary Endpoint CP Network ID
 .D.... NVSSCNM - Secondary Endpoint CP Name
 .D.... NVSSCNT - Secondary Endpoint CP Network ID
 .DWM.. PLDOMAIN - PLU Domain Name
 .DWM..E PLU - Primary Logical Unit
 .DWM.. PLUSAPU - PLU Subarea Physical Unit
 .DWM.. PRODUCT - Network Product (Source) Name
 .DWM..E SAMPLES - Number of Samples
 .DWM.. SEStYPE - Session Type
 .DWM.. SLDOMAIN - SLU Domain Name
 .DWM..E STARTTS - Start Time Stamp
 .DWM.. TMOFFSET - Time Offset

Retained Data Elements

.DWM.. NLLCNTR - Objective Counter Number
 .D.... NLLCOS - Class of Service
 .D.... NLLExRTE - Explicit Route Number
 .DWM.. NLLPCOBJ - Objective Percentage
 .DWM.. NLLRDEF - Response Definition
 .DWM.. NLLROBTM - Objective Response Time
 .D.... NLLRVER - Reverse Explicit Route Number
 .D.... NLLTRPTy - Transmission Priority
 .D.... NLLVR RTE - Virtual Route Number
 .D.... NLLXNET - Cross-network Session (Y or N)

Accumulated Data Elements

.DWM..E NLLNRCBR - Number Control Bytes Received
 .DWM..E NLLNRCBS - Number Control Bytes Sent
 .DWM..E NLLNRCPR - Number Control PIUs Received

.DWM..E NLLNRCPS - Number Control PIUs Sent
.DWM..E NLLNRROM - Number of Times Resp Obj Met
.DWM..E NLLNRTBR - Number Text Bytes Received
.DWM..E NLLNRTBS - Number Text Bytes Sent
.DWM..E NLLNRTPR - Number Text PIUs Received
.DWM..E NLLNRTPS - Number Text PIUs Sent
.DWM..E NLLRDST1 - Response Dist Count 1 (Boundary A)
.DWM..E NLLRDST2 - Response Dist Count 2 (Boundary B)
.DWM..E NLLRDST3 - Response Dist Count 3 (Boundary C)
.DWM..E NLLRDST4 - Response Dist Count 4 (Boundary D)
.DWM..E NLLRDST5 - Response Dist Count 5 (Above A,B,C,D)
.DWM..E NLLTRES - Response Event Count
.DWM..E NLLTRSTM - Total Response Time

Derived Data Elements

.DW... NLLAVCBR - Average Bytes per PIU Recvd (Control)
.DW... NLLAVCBS - Average Bytes per PIU Sent (Control)
.DW... NLLAVTBR - Average Bytes per PIU Recvd (Text)
.DW...E NLLAVTBS - Average Bytes per PIU Sent (Text)
.DWM..E NLLAVTTM - Average Total Response Time
.DWM..E NLLPCOBM - Pct of Times Response Obj Met
.DWM..E NLLPCTR1 - Cum. Pct All Resp Within Limit 1
.DWM..E NLLPCTR2 - Cum. Pct All Resp Within Limit 2
.DWM..E NLLPCTR3 - Cum. Pct All Resp Within Limit 3
.DWM..E NLLPCTR4 - Cum. Pct All Resp Within Limit 4

5.3.4.3 Usage Considerations

This section identifies special considerations or techniques related to using the NVSNLL File. In addition, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &ddiit, where d is the database identifier, iit is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. The NLDM System Activity (NVSLSY) File and the NLDM Link Activity (NVSNLL) File combine data from two separate collection functions within the same monitor. That is, these files either combine two collection functions within IBM Tivoli NetView Performance Monitor or two collection functions within CA NetMaster.

From NetView, this file combines data from the RTM and A&A data collection functions. If both functions are turned on in NetView, then RTM and A&A data is automatically forwarded to NetView and combined in a session termination record, even if the data is not actively solicited via COLLECT and RECORD commands.

From CA NetMaster, this file combines data from the Network Tracking System component (NTS) RTM collection function and the accounting data collection function.

You must ensure that these two data collection functions are synchronized or the data from the two functions in each file represent information from different time periods.

To synchronize NetView Response Time Monitor (RTM) data and NetView accounting and availability (A&A) data collection, execute the NetView COLLECT and NetView RECORD commands simultaneously at regular intervals throughout the day via NetView/NCCF CLISTs. (See Chapter 6 for a

discussion of the sample CLISTs shipped with NetView for the COLLECT and RECORD commands.)

- o The NetView COLLECT command produces the SMF type 39 interval record that contains RTM data.
- o The NetView RECORD command produces the the SMF type 39 interval record that contains A&A data.

On NetView hosts that control large network domains, you may not be able to synchronize the collection of RTM and A&A data on a domain-wide basis. For example, if a NetView domain contains 2,000 or more remote 3274/3174 cluster controllers with the RTM feature, several minutes may elapse from the time the NetView COLLECT command executes until the time NetView receives RTM data from all of the remote controllers. A similar delay does not occur when A&A data is received because it is extracted internally from VTAM.

A possible solution is to synchronize the collection of A&A and RTM data for a subset of network resources within a NetView domain. For example, if you want to use the data as it is organized in the NLDM Link Activity (NVSNULL) File, synchronize execution of the NetView COLLECT and RECORD commands for all the resources attached to a given NCP or link. If the arrangement of data in the NLDM System Activity (NVSLSY) File is more useful to your data center, synchronize collection of the A&A and RTM data by primary logical unit (PLU).

For information on how to synchronize RTM data collection and accounting data collection from the Network Tracking System (NTS) and the Network Error Warning System (NEWS), two components of CA NetMaster Network Management for SNA, see the CA NetMaster NM for SNA Getting Started guide, Administration Guide, and other documentation.

2. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - HOUR should not be used in MONTHS.
 - DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - WEEKS should not be used in MONTHS.
3. The following data elements are user-defined. The value

in each depends on user-selected options or user-supplied SAS code:

- o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
- o TMOFFSET - TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

4. The following data elements lose significance once summarization has been performed. These data elements should only be referenced when the last observed value in a summarization interval is significant.

NLDMVRR - NLDM Version and Release ID
 NLDVAL1 - NLDM Response Distribution Limits 1
 NLDVAL2 - NLDM Response Distribution Limits 2
 NLDVAL3 - NLDM Response Distribution Limits 3
 NLDVAL4 - NLDM Response Distribution Limits 4
 PLDOMAIN - PLU Domain Name
 PLU - Primary Logical Unit
 PLUSAPU - PLU Subarea Physical Unit
 SLDOMAIN - SLU Domain Name
 SESTYPE - Session Type
 SLU - Secondary Logical Unit
 SLUPU - SLU Physical Unit
 TMOFFSET - TIME OFFSET
 NLLCNTR - Objective Counter Number
 NLLCOS - Class of Service
 NLLXRTE - Explicit Route Number
 NLLPCOBJ - Objective Percentage
 NLLRDEF - Response Definition
 NLLROBTM - Objective Response Time
 NLLRVER - Reverse Explicit Route Number
 NLLTRPTY - Transmission Priority
 NLLVRTE - Virtual Route Number
 NLLXNET - Cross-network Session

Retrieval Example

Report the total connect time for all sessions on each link during prime shift yesterday.

```
/* SET THE SUMMARY BY AND BREAK MACROS */
%LET BY = NETWRKID SYSID SLUSAPU SLULINK;
%LET BREAK = SLULINK;

DATA SUMMED;
SET &PNVSD..NVSNLL01;
IF 9 GE HOUR LE 17; /* SELECT PRIME SHIFT */

PROC SORT DATA=SUMMED OUT=SORTED;BY &BY;

DATA SUMMED (RENAME=(DURATION=ACTIVE SLUSAPU=NCP));
SET SORTED;
%NLLSUM;          /* SUM THE DATA */
RUN;

PROC PRINT; VAR SLULINK ACTIVE;
BY NETWRKID SYSID NCP;
TITLE
'DAYS NVSNLL01, PRIME SHIFT LINK SESSION CONNECT TIME';
RUN;
```

5.3.5 NLDM Route File (NVS RTE)

The NLDM Route File (NVS RTE) quantifies the connect time and total characters transmitted for each virtual route and identifies the route elements and transmission groups associated with each virtual route by user-defined account code.

This file is derived from the NetView Session Monitor/NLDM External Log record.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.3.5.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	RTEVRRTE	SESTYPE	YEAR	
	MONTH	DAY	HOUR	ENDTS		
DAYS	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	RTEVRRTE	SESTYPE	YEAR	
	MONTH	DAY	HOUR			
WEEKS	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	RTEVRRTE	SESTYPE	YEAR	
	WEEK	ZONE	HOUR			
MONTHS	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	RTEVRRTE	SESTYPE	YEAR	
	MONTH	ZONE				
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not

is controlled by the complex definition of the
DERIVED option.

Figure 5-21. NVSRTE Timespan Granularity Chart

5.3.5.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

X - DETAIL
 D - DAYS
 W - WEEKS
 M - MONTHS
 Y - YEARS
 T - TABLES AREA
 . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E DAY - Day of Month
 XDW...E HOUR - Hour of Day
 XD.M..E MONTH - Month of Year
 XDWM..E NETWRKID - Network Identifier
 XDWM..E RTEVRRTE - Virtual Route Number
 XDWM..E SESTYPE - Session Type

XDWM..E SNTACT1 - PRIMARY LOGICAL UNIT(PLU)
XDWM..E SNTACT2 - SLUSAPU NETV/NPM1.3,SLUSA NPM1.2 OR NSPY
XDWM..E SNTACT3 - SLUPU IF NLDM OR NETSPY, SLU IF NPM
XDWM..E SNTACT4 - NLDM PERFCLSS, NPM BLANK, NSPY/NAC SLU
XDWM..E SNTACT5 - NOT-USED
XDWM..E SYSID - System Identifier
XDW...E WEEK - Week of Year
XDWM..E YEAR - Year of Century
XDWM..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
XDWM.. DURATION - Recording Interval Time
XDWM..E ENDTS - End Time Stamp
XDWM.. MICSVER - CA MICS Version Number
XD.... NLDMVRR1 - NLDM Version and Release Id
X..... NVSPRNM - Primary Endpoint CP Name
X..... NVSPRNT - Primary Endpoint CP Network ID
X..... NVSSCNM - Secondary Endpoint CP Name
X..... NVSSCNT - Secondary Endpoint CP Network ID
X.....E ORGSYSID - Originating System Identification
XD....E PLU - Primary Logical Unit
XDWM.. PRODUCT - Network Product (Source) Name
X.....E SLU - Secondary Logical Unit
XD....E SLULINK - SLU Link
XDWM..E STARTTS - Start Time Stamp
XD.... TMOFFSET - Time Offset
X.....E USESSIDC - Unique Session ID (Character)

Retained Data Elements

XDWM..E RTEELNA1 - Route Element 1 Name
XDWM..E RTEELNA2 - Route Element 2 Name
XDWM..E RTEELNA3 - Route Element 3 Name
X..... RTENRRE - Number of Route Elements in Table
X..... RTENRTRE - Total No. Route Elements Traversed
XDWM.. RTETGNM1 - Transmission Group (out) 1
XDWM.. RTETGNM2 - Transmission Group (out) 2
XDWM.. RTETGNM3 - Transmission Group (out) 3
XD.... RTEXDMN - Cross-domain Session (Y or N)

Accumulated Data Elements

X..... RTECONTM - Connect Time
XDWM..E RTENRTCH - Total Characters Transmitted

5.3.5.3 Usage Considerations

This section identifies special considerations or techniques related to using the NVSRTE File. In addition, a retrieval example is provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Determining Number of Route Element/TG Names

Although the NLDM Route (NVS RTE) File can carry up to nine route element names (RTEELN_x) and nine transmission group names (RTETGNM_x) in each observation, the file is shipped with only three route element names (RTEELN1 - RTEELN3) and three transmission group names (RTETGNM1 - RTETGNM3) activated to minimize its size. If a significant number of logical unit to logical unit (LU-LU) sessions in your network span more than three route elements or transmission groups, you may wish to increase the number of route element and transmission group names in the NVSRTE file.

A simple way to determine if this increase is necessary is to examine the content of the element Number of Route Elements in Table (RTENRRE). If the value of this element is greater than three for a large number of the virtual routes in your network, you should increase the number of route element and transmission group names in the file.

You can change the number of RTEELN_x and RTETGNM_x members in each observation in the NLDM Route File by modifying the RTEELN_x and RTETGNM_x statements in the SNTGENIN member in sharedprefix.MICS.GENLIB. Refer to Chapter 6 in the CA MICS System Modification Guide for complete instructions. In the example below, the number of route element names is increased from three to four by activating Route Element 4 Name. To accomplish this,

- o Modify the name statement for RTEELNA4 in sharedprefix.MICS.GENLIB(SNTGENIN) by replacing each N with 0 in the DETAIL, DAYS, WEEKS, and MONTHS timespans, and
- o Run the component generator for the CA MICS Network Analyzer Option.
- o RTEELNA4 before the change (inactive in all timespans)

```
                                TIME-SPAN
                                X D W M Y
                                -----
ALIAS RTEELNAX
NAME RTEELNA4      00  N N N N N  Route Element 4 Name
```

- o RTEELNAX after the change (active in DETAIL, DAYS, WEEKS, and MONTHS timespans)

```
                                TIME-SPAN
                                X D W M Y
                                -----
ALIAS RTEELNAX
NAME RTEELNA4      00  0 0 0 0 N  Route Element 4 Name
```

Note: Replacing N with 0 in the YEARS timespan would have no effect because the NLDM Route File is not supported in the YEARS timespan. Route Element 4 Name must be activated in the DETAIL timespan if it is to be activated in any of the higher timespans. The value of the RTEELNAX in the higher timespans is derived from its value in the DETAIL timespan.

NetView does not necessarily record the names of all of the route elements traversed in the route element table. In some cases, one or more of the route elements will be defined in the configuration data portion of the SMF type 39 records and will not be restated in the route element table. The CA MICS data element RTENRRE reflects the number of elements defined in the route element table. To know the actual number of route elements traversed, refer to the CA MICS data element RTENRTRE, Total Number of Route Elements Traversed.

2. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.

- o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEKS should not be used in MONTHS.
- 3 The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
- o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.
4. The following data elements lose significance once summarization has been performed, unless they are used in the summarization sequence as a result of being included in one of the accounting fields (i.e., SNTACT1, SNTACT2, etc.).
- NLDMVRR - NLDM Version and Release ID
 - PLU - Primary Logical Unit
 - SLU - Secondary Logical Unit
 - SLULINK - SLU Link
 - TMOFFSET - TIME OFFSET
 - RTEELNAX - Route Element x Name
 - RTETGNMx - Transmission Group (out) x
 - RTEXDMN - Cross-domain Session (Y or N)
5. For TSO sessions, both NetView and CA NetMaster record multiple values for the primary logical unit (PLU) for sessions with a single TSO system. These duplicate values are carried over into the CA MICS data for TSO sessions in the element PLU. This can greatly increase the size of the file if PLU is chosen as one of the account codes. This problem can be circumvented by the user-coded routine in prefix.MICS.PARMS(SNTPLURT), which sets the multiple values for PLU to a single value for each TSO system. Refer to Section 7.10 for information about SNTPLURT.

6. If you are processing CA NetSpy Virtual Route Activity data, you should also look at the SNTNVR file for response time information for the virtual route.

Retrieval Example

Show connect time by virtual route number using the data from yesterday.

```
/* SET THE SUMMARY MACROS */
%LET BY = NETWKID SYSID RTEVRRTE;
%LET BREAK = RTEVRRTE;

PROC SORT DATA=&PSNTX..NVS RTE01 OUT=SORTED;BY &BY;

DATA SUMMED (RENAME=(RTECONTM=ACTIVE));
SET SORTED;
%RTESUM;          /* SUM THE DATA */
RUN;

PROC PRINT; VAR RTEVRRTE ACTIVE;
BY NETWKID SYSID;
TITLE 'DETAIL NVS RTE01, VIRTUAL ROUTE CONNECT TIME';
RUN;
```

5.3.6 NLDM Response Time File (NVSRTM)

The NLDM Response Time File (NVSRTM) quantifies network service (response time) received, including average response times and response distribution percentages by user-defined account code.

This file is derived from the Response Time Monitor (RTM) data in either the NetView Session Monitor/NLDM External Log Record or the CA NetMaster NTS SMF Record.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.3.6.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	YEAR	MONTH	DAY	
	HOUR	ENDTS				
DAYS	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	YEAR	MONTH	DAY	
	HOUR					
WEEKS	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	YEAR	WEEK	ZONE	
	HOUR					
MONTHS	NETWRKID	SYSID	SNTACT1	SNTACT2	SNTACT3	
	SNTACT4	SNTACT5	YEAR	MONTH	ZONE	
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not

is controlled by the complex definition of the
DERIVED option.

Figure 5-22. NVSRTM Timespan Granularity Chart

5.3.6.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

X - DETAIL
D - DAYS
W - WEEKS
M - MONTHS
Y - YEARS
T - TABLES AREA
. - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XDW...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	SNTACT1	- PRIMARY LOGICAL UNIT(PLU)
XDWM..E	SNTACT2	- SLUSAPU NETV/NPM1.3,SLUSA NPM1.2 OR NSPY
XDWM..E	SNTACT3	- SLUPU IF NLDM OR NETSPY, SLU IF NPM

XDWM..E SNTACT4 - NLDM PERFCLSS, NPM BLANK, NSPY/NAC SLU
XDWM..E SNTACT5 - NOT-USED
XDWM..E SYSID - System Identifier
XDW...E WEEK - Week of Year
XDWM..E YEAR - Year of Century
XDWM..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
XDWM.. DURATION - Recording Interval Time
XDWM..E ENDTS - End Time Stamp
XDWM.. MICSVER - CA MICS Version Number
X..... NETGROUP - Network Service Group
XDWM.. NLDMVRRL - NLDM Version and Release Id
XDWM..E NLDRVAL1 - NLDM Response Distribution Limits 1
XDWM..E NLDRVAL2 - NLDM Response Distribution Limits 2
XDWM..E NLDRVAL3 - NLDM Response Distribution Limits 3
XDWM..E NLDRVAL4 - NLDM Response Distribution Limits 4
X..... NVSPRNM - Primary Endpoint CP Name
X..... NVSPRNT - Primary Endpoint CP Network ID
X..... NVSSCNM - Secondary Endpoint CP Name
X..... NVSSCNT - Secondary Endpoint CP Network ID
XD....E PERFCLSS - Performance Class (NLDM)
XD.... PLU - Primary Logical Unit
XDWM.. PRODUCT - Network Product (Source) Name
XDWM..E SAMPLES - Number of Samples
XDWM.. SESTYPE - Session Type
XD....E SLU - Secondary Logical Unit
XD.... SLULINK - SLU Link
XDWM..E STARTTS - Start Time Stamp
XDWM.. TMOFFSET - Time Offset
X..... USESSIDC - Unique Session ID (Character)

Retained Data Elements

XDWM..E RTMCNTR - Objective Counter Number
XDWM..E RTMPCOBJ - Objective Percentage
XDWM.. RTMRDEF - Response Definition
XDWM.. RTMRBTM - Objective Response Time
XD.... RTMXDMN - Cross-domain Session (Y or N)

Accumulated Data Elements

XDWM.. RTMCOST - Billable Cost
XDWM..E RTMNRROM - Number of Times Resp Obj Met
XDWM..E RTMRDST1 - Response Dist Count 1 (Boundary A)
XDWM..E RTMRDST2 - Response Dist Count 2 (Boundary B)
XDWM..E RTMRDST3 - Response Dist Count 3 (Boundary C)

XDWM..E RTMRDST4 - Response Dist Count 4 (Boundary D)
XDWM..E RTMRDST5 - Response Dist Count 5 (Above A,B,C,D)
XDWM..E RTMTRESC - Total Response Event Count
XDWM..E RTMTRSTM - Total Response Time

Derived Data Elements

XDWM..E RTMAVTTM - Average Total Response Time
XDWM..E RTMPCOBM - Pct of Times Response Obj Met
XDWM..E RTMPCTR1 - Cum. Pct All Resp Within Limit 1
XDWM..E RTMPCTR2 - Cum. Pct All Resp Within Limit 2
XDWM..E RTMPCTR3 - Cum. Pct All Resp Within Limit 3
XDWM..E RTMPCTR4 - Cum. Pct All Resp Within Limit 4

5.3.6.3 Usage Considerations

This section identifies special considerations or techniques related to using the NVSRTM File. In addition, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &ddiit, where d is the database identifier, iit is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. To ensure that the NVSRTM file's response time information is meaningful above the DETAIL timespan, be sure that PERFCLSS is defined in an account code for this file.
2. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - HOUR should not be used in MONTHS.
 - DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - WEEKS should not be used in MONTHS.
3. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is

assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

4. The following data elements lose significance once summarization has been performed, unless they are used in the summarization sequence as a result of being included in one of the accounting fields (i.e., SNTACT1, SNTACT2, etc.).

NLDMVRR - NLD Version and Release ID
 NLDRVAL1 - NLD Response Distribution Limits 1
 NLDRVAL2 - NLD Response Distribution Limits 2
 NLDRVAL3 - NLD Response Distribution Limits 3
 NLDRVAL4 - NLD Response Distribution Limits 4
 PERFCLSS - Performance Class (NLD)
 PLU - Primary Logical Unit
 SLU - Secondary Logical Unit
 SLULINK - SLU Link
 TMOFFSET - TIME OFFSET
 RTMCNTR - Objective Counter Number
 RTMPCOBJ - Objective Percentage
 RTMRDEF - Response Definition
 RTMROBTM - Objective Response Time
 RTMXDMN - Cross-domain Session (Y or N)

5. For TSO sessions, both NetView and CA NetMaster record multiple values for the primary logical unit (PLU) for sessions with a single TSO system. These duplicate values are carried over into CA MICS data for TSO sessions in the element PLU. The duplicate PLU values can greatly increase the size of the file if PLU is chosen as one of the account codes.

This problem can be circumvented by the user-coded routine in prefix.MICS.PARMS(SNTPLURT), which sets the multiple values for PLU to a single value for each TSO system. Refer to Section 7.10 for information about SNTPLURT.

Retrieval Examples

1. Assume that the data center response time objectives state that 90 percent of all total responses must be less than five seconds and that NLD is parameterized for Performance Class (PERFCLSS) 'TSO' so that NLDRVAL2 (response time limit bucket 2) is set at five seconds. Select those sessions that do not meet the stated objective. List each session and any relevant information.

```
DATA WKFILE
  (RENAME=(PLU=APPL SLU=TERMINAL RTMAVTTM=RESPONSE
    RTMPCOBM=PCT_MET));
SET &PNVSX..NVSRTM01;
IF PERFCLSS = 'TS0';
IF RTMPCTR2 LT 90; /* SELECT LESS THAN 90 % */
  PROC PRINT DATA=WKFILE;
BY NETWRKID SYSID;
VAR APPL SLULINK TERMINAL RESPONSE PCT_MET;
TITLE 'RESPONSE OBJECTIVE # 3 LESS THAN 90 %';
RUN;
```

2. Produce a report showing by hour those applications missing their response objectives using today's data.

```
DATA WKFILE (RENAME=(PLU=APPL));
SET &PNVSX..NVSRTM01;
IF RTMNRROM=0; /* =1 IN DETAIL IF OBJ MET */

PROC FREQ DATA=WKFILE;
TABLES APPL * HOUR / NOROW NOCOL NOCUM;
TITLE 'DETAIL NVSRTM01, RESPONSE OBJECTIVE MISSED';
RUN;
```

5.3.7 NLDM VTAM BIND Failure File (NVSVBF)

The NLDM VTAM Bind Failure File (NVSVBF) quantifies the number of sessions that failed due to abnormal VTAM UNBINDs. The data is summarized by failure code, failure type, session partners (PLU and SLU), and user-defined performance class.

This file is derived from either the NetView Session Monitor/NLDM External Log Record or the CA NetMaster NTS SMF Record.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.3.7.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	PERFCLSS	PLU	SLU	
	VBFFTYPE	VBFRCODE	YEAR	MONTH	DAY	
	HOUR	ENDTS				
DAYS	NETWRKID	SYSID	PERFCLSS	PLU	SLU	
	VBFFTYPE	VBFRCODE	YEAR	MONTH	DAY	
	HOUR					
WEEKS	NETWRKID	SYSID	PERFCLSS	PLU	SLU	
	VBFFTYPE	VBFRCODE	YEAR	WEEK	ZONE	
	HOUR					
MONTHS	NETWRKID	SYSID	PERFCLSS	PLU	SLU	
	VBFFTYPE	VBFRCODE	YEAR	MONTH	ZONE	
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not

is controlled by the complex definition of the
DERIVED option.

Figure 5-23. NVSVBF Timespan Granularity Chart

5.3.7.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

X - DETAIL
 D - DAYS
 W - WEEKS
 M - MONTHS
 Y - YEARS
 T - TABLES AREA
 . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E DAY - Day of Month
 XDW...E HOUR - Hour of Day
 XD.M..E MONTH - Month of Year
 XDWM..E NETWRKID - Network Identifier
 XDWM..E PERFCLSS - Performance Class (NLDM)
 XDWM..E PLU - Primary Logical Unit

XDW..E SLU - Secondary Logical Unit
XDW..E SYSID - System Identifier
XDW..E VBFFTYPE - VTAM Failure Type
XDW..E VBFRCODE - Unbind/Bind Failure Code
XDW...E WEEK - Week of Year
XDW..E YEAR - Year of Century
XDW..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
XDW.. DURATION - Recording Interval Time
XDW..E ENDTS - End Time Stamp
XDW.. MICSVER - CA MICS Version Number
XDW.. NLDMVRRL - NLDM Version and Release Id
X..... NVSPRNM - Primary Endpoint CP Name
X..... NVSPRNT - Primary Endpoint CP Network ID
X..... NVSSCNM - Secondary Endpoint CP Name
X..... NVSSCNT - Secondary Endpoint CP Network ID
XDW.. PRODUCT - Network Product (Source) Name
XDW.. SESTYPE - Session Type
XDW.. SLULINK - SLU Link
XDW..E STARTTS - Start Time Stamp
XDW.. TMOFFSET - Time Offset
X..... USESSIDC - Unique Session ID (Character)

Retained Data Elements

XDW..E VBFAUSE - Bind Failure/Unbind Reason
XD.... VBFXDMN - Cross-domain Session (Y or N)
XD.... VBFXNET - Cross-network Session (Y or N)

Accumulated Data Elements

XDW..E VBFNRBF - Number of Bind Failures

5.3.7.3 Usage Considerations

This section identifies special considerations or techniques related to using the NVSVBF File. In addition, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &ddiit, where d is the database identifier, iit is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher time-spans, certain fields lose significance and should not be used in those cases.
 - HOUR should not be used in MONTHS.
 - DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - WEEKS should not be used in MONTHS.
2. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one- to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS data base. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.
3. The following data elements lose significance once

summarization has been performed. These data elements should be referenced only when the last observed value in a summarization interval is significant.

NLDMVRRL - NLDM Version and Release ID
SESTYPE - Session Type
SLULINK - SLU Link
TMOFFSET - TIME OFFSET
VBFAUSE - BIND Failure/UNBIND Reason
VBFXDMN - Cross-domain Session (Y or N)
VBFXNET - Cross-network Session (Y or N)

4. For TSO sessions, both NetView and CA NetMaster record multiple values for the primary logical unit (PLU) for sessions with a single TSO system. These duplicate values are carried over into CA MICS data for TSO sessions in the element PLU. This can greatly increase the size of the file if PLU is chosen as one of the account codes. This problem can be circumvented by the user-coded CA MICS routine in prefix.MICS.PARMS(SNTPLURT), which sets the multiple values for PLU to a single value for each TSO system. Refer to Section 7.10 for information about SNTPLURT.

Retrieval Example

List the frequency of VTAM UNBIND codes by application from today's data.

```
PROC FREQ DATA=&PNVSX..NVSVBFO1;  
TABLES PERFCLSS * VBFCODE / NOROW NOCOL NOCUM;  
TITLE 'DETAIL NVSVBF01, PERF CLASS BY UNBIND CODE';  
RUN;
```


5.4 TCP Information Area

The TCP Information Area captures information about TCP/IP in the files described in this chapter:

- 1 - Telnet Server File (TCPSTN)
- 2 - Telnet Client File (TCPCTN)
- 3 - FTP Server File (TCPFSF)
- 4 - FTP Client File (TCPFCF)
- 5 - API Calls for Sockets File (TCPAPI)
- 6 - FTP Login Failure File (TCPFLF)
- 7 - IP Statistics File (TCPIPX)
- 8 - ICMP Statistics File (TCPICX)
- 9 - TCP Statistics File (TCPTCI)
- 10 - UDP Statistics File (TCPUDI)
- 11 - Storage Statistics File (TCPSTG)
- 12 - Interface Statistics File (TCPIFS)

5.4.1 Telnet Server File (TCPSTN)

The Telnet Server File (TCPSTN) quantifies TCP/IP Telnet server activity. The Telnet server provides a service to the client by transmitting data back and forth to the client.

This file is derived from SMF record types 118 and 119. In SMF 118, the Telnet Server data record is identified by characters 'LOGN' or 'LOGF' at offset 21. In SMF record type 119, it is the subtype 21 (TN3270 Telnet server SNA session termination record).

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.4.1.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	TCPIPHST	TCPRADDR	TCPLPORT	
	TCPRPORT	YEAR	MONTH	DAY	HOURL	
	ENDTS					
DAYS	NETWRKID	SYSID	TCPIPHST	YEAR	MONTH	
	DAY	HOURL				
WEEKS	NETWRKID	SYSID	TCPIPHST	YEAR	WEEK	
	ZONE					
MONTHS	NETWRKID	SYSID	TCPIPHST	YEAR	MONTH	
	ZONE					
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=DEFAULT option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-24. TCPSTN Timespan Granularity Chart

5.4.1.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XD...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	SYSID	- System Identifier
XDWM..E	TCPIPHST	- TCP/IP Host Name

X.....E TCPLPORT - Local Port Number (Data Connection)
 X.....E TCPRADDR - Remote IP Address (Data Connection)
 X.....E TCPRPORT - Remote Port Number (Data Connection)
 XDWM...E WEEK - Week of Year
 XDWM...E YEAR - Year of Century
 XDWM...E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
 X.....E DEVNUM - Device Number
 XDWM.. DURATION - Recording Interval Time
 XDWM..E ENDTS - End Time Stamp
 XDWM..E MICSVER - CA MICS Version Number
 XDWM..E PRODUCT - Network Product (Source) Name
 XDWM..E STARTTS - Start Time Stamp
 XDWM..E STNBYTEI - In Byte Count
 XDWM..E STNBYTEO - Out Byte Count
 XDWM..E SYSNAME - System Name
 XDWM..E SYSPLEX - Sysplex Name
 X.....E TCPIPTYP - TCP/IP Type
 X.....E TCPLADDR - Local IP Address (Data Connection)
 X.....E TCPSTACK - TCP/IP Stack Name
 XD....E TCPSTQN - TCP/IP Address Space Name
 X.....E TCPUID - User ID
 X.....E TCPVRRL - z/OS CS TCP/IP Version/Rel.
 XDWM.. TMOFFSET - Time Offset

Retained Data Elements

X.....E STNAPPL - Application Name
 X.....E STNCOPT - Telnet Connection Options Negotiated
 X.....E STNCOPT1 - TN3270E Connection Options 1
 X.....E STNCOPT2 - TN3270E Connection Options 2
 X.....E STNDTYPE - Telnet Device Type
 X.....E STNETS - Session Termination Timespan
 X.....E STNFLAG - Identification Flag
 X.....E STNIPMMT - Method Used to Measure IP Trip Time
 X.....E STNLMODE - SNA Logmode
 X.....E STNLU - Telnet LU Name
 X.....E STNLUSEL - TN3270E LU Selection Method
 X.....E STNRCODE - Session Termination Reason Code
 X.....E STNSSL - SSL Status
 X.....E STNSTS - Session Initiation Timespan
 X.....E STNSTYPE - Telnet Session Type

Accumulated Data Elements

XDWM..E STNIMMT - Master MonitorGroup Table Index

XDM..E STNIPRTT - Total IP RTT for this Session
XDM..E STNISRTT - Total of Square of Each IP RTT
XDM..E STNRTICT - Trans Used to Measure IP RTT Count
XDM..E STNRTTCT - Trans Used to Measure RTT Count
XDM..E STNSSRTT - Total of Square of Each SNA RTT
XDM..E STNTORTT - Total RTT for this Session
XDM..E STNTSRTT - Total of Square of Each RTT
XDM..E STNUBTM1 - Upper Boundary Time - Bucket 1
XDM..E STNUBTM2 - Upper Boundary Time - Bucket 2
XDM..E STNUBTM3 - Upper Boundary Time - Bucket 3
XDM..E STNUBTM4 - Upper Boundary Time - Bucket 4
XDM..E STNUPTC1 - Trans Meeting RTT Criteria 1 Count
XDM..E STNUPTC2 - Trans Meeting RTT Criteria 2 Count
XDM..E STNUPTC3 - Trans Meeting RTT Criteria 3 Count
XDM..E STNUPTC4 - Trans Meeting RTT Criteria 4 Count
XDM..E STNUPTC5 - Trans Meeting RTT GT Criteria 4 Count

Derived Data Elements

XDM..E STNAVIRT - Avg IP RTT for this Session
XDM..E STNAVRTT - Avg RTT for this Session

5.4.1.3 Usage Considerations

This section identifies special considerations or techniques related to using the TCPSTN file. In addition, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &ddiit, where d is the database identifier, iit is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. The Telnet Server File (TCPSTN) is built by selecting data from SMF record type SMF 118 and/or SMF record type 119. The data of type LOGN and LOGF from SMF type 118 records. An observation of type LOGN is matched with corresponding observations of type LOGF before storing it in the STN file. Any observation without an exact match is stored in the Telnet Suspend File (TCPTSS). Care must be exercised when combining observations from other TCP files to avoid duplication.

The data from SMF record type 119 subtype 21 (TN3270 Server SNA session termination record) is also used to populate this file. The TN3270 Server SNA session termination record contains the connection start time and connection end time, thereby eliminating the need to hold session start records in the suspend file to calculate the session duration.

Consult your z/OS CS system programmer to turn off SMF record type 118 and to activate SMF record type 119. This will improve your DAY056 job performance.

2. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.

- o WEEKS should not be used in MONTHS.
3. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
- o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.
4. The following data elements lose significance after summarization has been performed. These data elements should be referenced only when the last observed value in a summarization interval is significant.

TCPRPORT - Remote Port Number (Data Connection)
TCPLPORT - Local Port Number (Data Connection)
TCPRADDR - Remote IP Address (Data Connection)
TCPLADDR - Local IP Address (Data Connection)
TCPIPTYP - TCP/IP Type
TCPSTACK - TCP/IP Stack Name
DEVNUM - Device Number
TCPVRRL - z/OS CS TCP/IP Version/Rel.
TCPUID - User ID

Retrieval Example

Chart prime shift TCP/IP Telnet Server activity for Sysid
PROD. Use yesterday's data.

```
DATA SELECTED (KEEP=SYSID DAY ZONE HOUR STNBYTEI STNBYTEO)
;
SET &PTCPD..TCPSTN01;
IF SYSID = 'PROD';
IF 9 GE HOUR LE 17; /* SELECT PRIME SHIFT */

PROC CHART DATA=SELECTED;
  VBAR HOUR / SUMVAR=STNBYTEI
```



```
DISCRETE;  
TITLE1 'DAYS TCPSTN01, PRIME SHIFT IN BYTE COUNT ';  
RUN;
```

5.4.2 Telnet Client File (TCPCTN)

The Telnet Client File (TCPCTN) quantifies TCP/IP Telnet client activity. A Telnet client is a user of Telnet services provided by the server.

This file is derived from SMF record types 118 and 119. In SMF record 118, the Telnet Client data record is identified by characters 'LGON' or 'LGOF' at offset 21. In SMF record type 119, it is the subtype 23 (TSO Telnet client termination record).

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.4.2.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	TCPRADDR	TCPLPORT	TCPPRPORT	
	YEAR	MONTH	DAY	HOUR	ENDTS	
DAYS	NETWRKID	SYSID	YEAR	MONTH	DAY	
	HOUR					
WEEKS	NETWRKID	SYSID	YEAR	WEEK	ZONE	
MONTHS	NETWRKID	SYSID	YEAR	MONTH	ZONE	
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=DEFAult option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-25. TCPCTN Timespan Granularity Chart

5.4.2.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

- XD...E DAY - Day of Month
- XD...E HOUR - Hour of Day
- XD.M..E MONTH - Month of Year
- XDWM..E NETWRKID - Network Identifier
- XDWM..E SYSID - System Identifier
- X.....E TCPLPORT - Local Port Number (Data Connection)

X.....E TCPRADDR - Remote IP Address (Data Connection)
X.....E TCPRPORT - Remote Port Number (Data Connection)
XDWM...E WEEK - Week of Year
XDWM...E YEAR - Year of Century
XDWM...E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
XDWM.. DURATION - Recording Interval Time
XDWM...E ENDTS - End Time Stamp
XDWM...E MICSVER - CA MICS Version Number
XDWM...E PRODUCT - Network Product (Source) Name
X.....E STARTTS - Start Time Stamp
XDWM...E SYSNAME - System Name
XDWM...E SYSPLEX - Sysplex Name
X.....E TCPIPTYP - TCP/IP Type
X.....E TCPLADDR - Local IP Address (Data Connection)
X.....E TCPSTACK - TCP/IP Stack Name
XD....E TCPSTQN - TCP/IP Address Space Name
X.....E TCPUID - User ID
X.....E TCPVRL - z/OS CS TCP/IP Version/Rel.
XDWM.. TMOFFSET - Time Offset

Retained Data Elements

X.....E CTNCOPT - Telnet Connection Options Negotiated
X.....E CTNDTYPE - Telnet Device Type
X.....E CTNETS - Session Termination Timespan
X.....E CTNNODE - NJE Node Name
X.....E CTNSTS - Session Initiation Timespan

Accumulated Data Elements

XDWM...E CTNBYTEI - In Byte Count
XDWM...E CTNBYTEO - Out Byte Count

5.4.2.3 Usage Considerations

This section identifies special considerations or techniques related to using the TCPCTN file, as well as a retrieval example to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &ddiit, where d is the database identifier, iit is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &ddiit, where d is the database identifier, iit is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. The Telnet Client (TCPCTN) File is built by selecting data from SMF record type 118 and/or SMF record type 119. The data of type LGON and LGOF from SMF type 118 records. Care must be exercised when combining observations from other TCP files to avoid duplication.

The data from SMF record type 119 subtype 23 (TSO Telnet client connection termination record) is also used to populate this file. This record provides several new metrics that are not available in SMF 118 records.

Consult your z/OS CS system programmer to turn off SMF record type 118 and to activate SMF record type 119. This will improve your DAY056 job performance.

1. This file is really designed for use only at the DETAIL timespan. The following data elements lose significance once summarization has been performed, reducing the usability of this file.

- o CTNNODE - NJE Node Name
- o TCPIPTYP - TCP/IP Type
- o TCPLADDR - Local IP Address
- o TCPLPORT - Local Port Number
- o TCPRADDR - Remote IP Address
- o TCPRPORT - Remote Port Number

2. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:

- o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
- o TMOFFSET - TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

Retrieval Example

Report on the frequency of TCP/IP Telnet Client remote access for yesterday. This will report the type of activity which occurred, by Remote IP Address.

```
PROC FREQ DATA=&PTCPX.TCPCTN01 ;  
    TABLES TCPRADDR * TCPIPTYP / LIST;  
    TITLE1 'TCP/IP Activity By Remote Address';  
    RUN;
```

Report on the frequency of TCP/IP Telnet Client local access for yesterday. This will report the type of activity which occurred, by Local IP Address.

```
PROC FREQ DATA=&PTCPX.TCPCTN01 ;  
    TABLES TCPLADDR * TCPIPTYP / LIST;  
    TITLE1 'TCP/IP Activity By Local Address';  
    RUN;
```

5.4.3 FTP Server File (TCPFSF)

The File Transfer Protocol (FTP) Server File (TCPFSF) quantifies FTP server activity. The FTP server provides services to its client by transmitting data from host to client or host to host.

This file is derived from SMF record types 118 and 119. In SMF 118, the FTP Server data record is identified by characters other than 'LOGN', 'LOGF', 'LGON', 'LGOF', 'INIT', or 'TERM' at offset 21 and a character 'S' at offset 72. In SMF record type 119, it is the subtype 70 (FTP server completion record).

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.4.3.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	TCPIPHST	TCPRADDR	TCPLPORT	
	TCPRPORT	YEAR	MONTH	DAY	HOURL	
	ENDTS					
DAYS	NETWRKID	SYSID	TCPIPHST	YEAR	MONTH	
	DAY	HOURL				
WEEKS	NETWRKID	SYSID	TCPIPHST	YEAR	WEEK	
	ZONE					
MONTHS	NETWRKID	SYSID	TCPIPHST	YEAR	MONTH	
	ZONE					
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-26. TCPFSF Timespan Granularity Chart

5.4.3.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

X - DETAIL
 D - DAYS
 W - WEEKS
 M - MONTHS
 Y - YEARS
 T - TABLES AREA
 . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XD...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	SYSID	- System Identifier
XDWM..E	TCPIPHST	- TCP/IP Host Name

```

X.....E TCPLPORT - Local Port Number (Data Connection)
X.....E TCPRADDR - Remote IP Address (Data Connection)
X.....E TCPRPORT - Remote Port Number (Data Connection)
XDWM...E WEEK    - Week of Year
XDWM...E YEAR     - Year of Century
XDWM...E ZONE     - Time Zone

```

Common Data Elements

```

XD....E DAYNAME  - Name of Day of Week
XDWM.. DURATION - Recording Interval Time
XDWM..E ENDTS    - End Time Stamp
XDWM..E FSFBYTES - Bytes Count of Transmission
X.....E FSDFMT   - Data Format
X.....E FSFDSTYP - Dataset Type
XDWM..E FSFETM   - Transmission End Time
X.....E FSFMODE  - Transfer Mode
XDWM..E FSFSTM   - Transmission Start Time
X.....E FTPFSCP  - Control Connection Protection Level
X.....E FTPFSCS  - Cipher Specification
X.....E FTPFSDP  - Data Connection Protection Level
XDWM..E FTPFSLC  - Login Method is Certificate Count
XDWM..E FTPFSLP  - Login Method is Password Count
XDWM..E FTPFSLT  - Login Method is Kerberos Count
XDWM..E FTPFSMA  - Security Mechanism AT-TLS Count
XDWM..E FTPFSMG  - Security Mechanism GSSAPI Count
XDWM..E FTPFSMN  - Security Mechanism None Count
XDWM..E FTPFSMT  - Security Mechanism TLS Count
X.....E FTPFSPBS - Negotiated Protection Buffer Size
XDWM..E FTPID    - FTP ID (S-Server C-Client)
X.....E FTPLADRC - Local IP Address (Control Conn.)
X.....E FTPLPORC - Local Port Number (Control Conn.)
X.....E FTPRADRC - Remote IP Address (Control Conn.)
X.....E FTPRPORC - Remote Port Number (Control Conn.)
XDWM..E MICSVER  - CA MICS Version Number
XDWM..E PRODUCT  - Network Product (Source) Name
XDWM..E STARTTS  - Start Time Stamp
XDWM..E SYSNAME  - System Name
XDWM..E SYSPLEX  - Sysplex Name
X.....E TCPIPTYP - TCP/IP Type
X.....E TCPLADDR - Local IP Address (Data Connection)
XDWM..E TCPSSL2  - SSL Protocol V2 Count
XDWM..E TCPSSL3  - SSL Protocol V3 Count
X.....E TCPSTACK - TCP/IP Stack Name
XD....E TCPSTQN  - TCP/IP Address Space Name
XDWM..E TCPTLS1  - TLS Protocol V1 Count
X.....E TCPUID   - User ID
X.....E TCPVRL   - z/OS CS TCP/IP Version/Rel.
XDWM.. TMOFFSET  - Time Offset

```

Retained Data Elements

X.....E FSFABEND - Abnormal end Code
X.....E FSFCIDCC - TCP Conn. ID of FTP Control Connection
X.....E FSFCIDDC - TCP Conn. ID of FTP Data Connection
X.....E FSFDSN1 - Dataset Name / User ID
X.....E FSFDSN2 - Second Dataset Name
X.....E FSFETS - Transmission End Timespan
X.....E FSFFILTP - File Type
X.....E FSFHFS1 - HFS File Name 1
X.....E FSFHFS2 - HFS File Name 2
X.....E FSFLRPLY - Last Reply Sent to This Client
X.....E FSFMEM1 - Member Name for PDS
X.....E FSFMEM2 - Second PDS Member
X.....E FSFSESID - FTP Activity Logging Session ID
X.....E FSFSTRUC - Data Structure
X.....E FSFSTS - Transmission Start Timespan
X.....E FSFUID - Local User ID
X.....E FSFUIDF - User ID for Failed Logon Attempt

5.4.3.3 Usage Considerations

This section identifies special considerations or techniques related to using the TCPFSF file. In addition, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. FTP Server File (TCPFSF)	FTP Client File (TCPFCF)
-----	-----
SMF 118 FTP Server record FTP ID = 'S' at offset 72	SMF 118 FTP Client record FTP ID = 'C' at offset 72
SMF 119 subtype 70 (FTP Server completion record)	SMF 119 subtype 3 (FTP Client completion record)

Care must be exercised when analyzing any FTP command data which is the result of FTP data transfer from one MVS system to another within one domain. A SMF type 118 record is logged into both the originating host and the destination host. The originator host logs an entry as Client and the destination host logs the same entry as Server. However, these log records represent different domains.

- Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEKS should not be used in MONTHS.
- The following data elements are user-defined. The value in each depends on user-selected options or user-supplied

SAS code:

- o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
- o TMOFFSET - TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

4. The following data elements lose significance after summarization has been performed. These data elements should be referenced only when the last observed value in a summarization interval is significant.

TCPRPORT - Remote Port Number (Data Connection)
 TCPLPORT - Local Port Number (Data Connection)
 TCPRADDR - Remote IP Address (Data Connection)
 TCPLADDR - Local IP Address (Data Connection)
 TCPSTACK - TCP/IP Stack Name
 TCPSOCID - TCP Socket Resource ID
 TCPSOCNM - TCP Socket Resource Name
 TCPVRR - z/OS CS TCP/IP Version/Rel.
 TCPUID - User ID
 FSDFMT - Data Format
 FSFMODE - Transfer Mode
 FSFDSTYP - Dataset Type
 FTPRPORT - Remote Port Number (Control Conn.)
 FTPLPORT - Local Port Number (Control Conn.)
 FTPRADDR - Remote IP Address (Control Conn.)
 FTPLADDR - Local IP Address (Control Conn.)
 FTPFSCS - Cipher Specification for AT-TLS
 FTPFSPBS - Negotiated Protection Buffer Size
 FTPFSCP - Control Connection Protection Level
 FTPFSDP - Data Connection Protection Level

Retrieval Example

Chart prime shift FTP Server activity for sysid PROD. Use yesterday's data.

DATA SELECTED (KEEP=SYSID DAY ZONE HOUR FSFBYTEI FSFBYTES)

```
;
SET &PTCPD..TCPFSF01;
IF SYSID = 'PROD';
IF 9 GE HOUR LE 17; /* SELECT PRIME SHIFT */

PROC CHART DATA=SELECTED;
  VBAR HOUR / SUMVAR=FSFBYTES
  DISCRETE;
TITLE 'DAYS TCPFSF01, PRIME SHIFT IN BYTE COUNT ';
RUN;
```

5.4.4 FTP Client File (TCPFCF)

The File Transfer Protocol (FTP) Client File (TCPFCF) quantifies FTP client activity. A FTP client is a user of services provided by the FTP server.

This file is derived from SMF record types 118 and 119. In SMF 118, the FTP client data record is identified by characters other than 'LOGN', 'LOGF', 'LGON', 'LGOF', 'INIT', or 'TERM' at offset 21 and a character 'C' at offset 69. In SMF record type 119, it is the subtype 3 (FTP client completion record).

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.4.4.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

+-----+-----+-----+-----+-----+-----+-----+						
Timespan	Level of Data Granularity					
+-----+-----+-----+-----+-----+-----+-----+						
DETAIL	NETWRKID	SYSID	TCPIPHST	TCPRADDR	TCPLPORT	
	TCPRPORT	YEAR	MONTH	DAY	HOUR	
	ENDTS					
DAYS	NETWRKID	SYSID	TCPIPHST	YEAR	MONTH	
	DAY	HOUR				
WEEKS	NETWRKID	SYSID	TCPIPHST	YEAR	WEEK	
	ZONE					
MONTHS	NETWRKID	SYSID	TCPIPHST	YEAR	MONTH	
	ZONE					
YEARS	N/A					
+-----+-----+-----+-----+-----+-----+-----+						
TABLES	N/A					
+-----+-----+-----+-----+-----+-----+-----+						

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=DEFAult option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-27. TCPFCF Timespan Granularity Chart

5.4.4.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

X - DETAIL
D - DAYS
W - WEEKS
M - MONTHS
Y - YEARS
T - TABLES AREA
. - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD....E	DAY	- Day of Month
XD....E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	SYSID	- System Identifier
XDWM..E	TCPIPHST	- TCP/IP Host Name

```

X.....E TCPLPORT - Local Port Number (Data Connection)
X.....E TCPRADDR - Remote IP Address (Data Connection)
X.....E TCPRPORT - Remote Port Number (Data Connection)
XDWM...E WEEK    - Week of Year
XDWM...E YEAR    - Year of Century
XDWM...E ZONE    - Time Zone

```

Common Data Elements

```

XD....E DAYNAME  - Name of Day of Week
XDWM.. DURATION - Recording Interval Time
XDWM..E ENDTS    - End Time Stamp
XDWM..E FCFBYTES - Bytes Count if Applicable
X.....E FCFDFMT - Data Format
X.....E FCFDSTYP - Dataset Type
XDWM..E FCFETM   - Transmission End Time
X.....E FCFMODE  - Transfer Mode
XDWM..E FCFSTM   - Transmission Start Time
X.....E FTPFSCP  - Control Connection Protection Level
X.....E FTPFSCS  - Cipher Specification
X.....E FTPFSDP  - Data Connection Protection Level
XDWM..E FTPFSLC  - Login Method is Certificate Count
XDWM..E FTPFSLP  - Login Method is Password Count
XDWM..E FTPFSLT  - Login Method is Kerberos Count
XDWM..E FTPFSMA  - Security Mechanism AT-TLS Count
XDWM..E FTPFSMG  - Security Mechanism GSSAPI Count
XDWM..E FTPFSMN  - Security Mechanism None Count
XDWM..E FTPFSMT  - Security Mechanism TLS Count
X.....E FTPFSPBS - Negotiated Protection Buffer Size
XDWM..E FTPID    - FTP ID (S-Server C-Client)
X.....E FTPLADRC - Local IP Address (Control Conn.)
X.....E FTPLPORC - Local Port Number (Control Conn.)
X.....E FTPRADRC - Remote IP Address (Control Conn.)
X.....E FTPRPORC - Remote Port Number (Control Conn.)
XDWM..E MICSVER  - CA MICS Version Number
XDWM..E PRODUCT  - Network Product (Source) Name
XDWM..E STARTTS  - Start Time Stamp
XDWM..E SYSNAME  - System Name
XDWM..E SYSPLEX  - Sysplex Name
XDWM..E TCPIPTYP - TCP/IP Type
X.....E TCPLADDR - Local IP Address (Data Connection)
XDWM..E TCPSSL2  - SSL Protocol V2 Count
XDWM..E TCPSSL3  - SSL Protocol V3 Count
X.....E TCPSTACK - TCP/IP Stack Name
XDWM..E TCPTLS1  - TLS Protocol V1 Count
X.....E TCPUID   - User ID
X.....E TCPVRRL  - z/OS CS TCP/IP Version/Rel.
XDWM.. TMOFFSET - Time Offset

```

Retained Data Elements

X.....E FCFABEND - Abnormal end Code
X.....E FCFCIDCC - TCP Conn. ID of FTP Control Connection
X.....E FCFCIDDC - TCP Conn. ID of FTP Data Connection
X.....E FCFDSN1 - Local Data Set
X.....E FCFDSN2 - Local Directory/Second Data Set Name
X.....E FCFETS - Transmission End Timespan
X.....E FCFFILTP - File Type
X.....E FCFHFS1 - HFS File Name 1
X.....E FCFLRPLY - Reply to FTP Command
X.....E FCFMEM1 - Member Name for PDS
X.....E FCFSADDR - SOCKS IP Address
X.....E FCFSOCVR - SOCKS Version Number
X.....E FCFSOVR - SOCKS Port Number
X.....E FCFSTRUC - Data Structure
X.....E FCFSTS - Transmission Start Timespan
X.....E FCFUID - Remote User ID
X.....E FCFUID - User ID of User of FTP

5.4.4.3 Usage Considerations

This section identifies special considerations or techniques related to using the TCPFCF file. In addition, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &ddiit, where d is the database identifier, iit is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. FTP Server File (TCPFSF)	FTP Client File (TCPFCF)
-----	-----
SMF 118 FTP Server record FTP ID = 'S' at offset 72	SMF 118 FTP Client record FTP ID = 'C' at offset 72
SMF 119 subtype 70 (FTP Server completion record)	SMF 119 subtype 3 (FTP Client completion record)

Care must be exercised when analyzing any FTP command data which is the result of FTP data transfer from one MVS system to another within one domain. A SMF type 118 record is logged into both the originating host and the destination host. The originator host logs an entry as Client and the destination host logs the same entry as Server. However, these log records represent different domains.

- Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEKS should not be used in MONTHS.
- The following data elements are user-defined. The value in each depends on user-selected options or user-supplied

SAS code:

- o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
- o TMOFFSET - TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

4. The following data elements lose significance after summarization has been performed. These data elements should be referenced only when the last observed value in a summarization interval is significant.

TCPRPORT - Remote Port Number (Data Connection)
 TCPLPORT - Local Port Number (Data Connection)
 TCPRADDR - Remote IP Address (Data Connection)
 TCPLADDR - Local IP Address (Data Connection)
 TCPSTACK - TCP/IP Stack Name
 TCPSOCID - TCP Socket Resource ID
 TCPSOCNM - TCP Socket Resource Name
 TCPVRR - z/OS CS TCP/IP Version/Rel.
 TCPUID - User ID
 FCFDFMT - Data Format
 FCFMODE - Transfer Mode
 FCFDSTYP - Dataset Type
 FTPRPORT - Remote Port Number (Control Conn.)
 FTPLPORT - Local Port Number (Control Conn.)
 FTPRADRC - Remote IP Address (Control Conn.)
 FTPLADRC - Local IP Address (Control Conn.)
 FTPFSCS - Cipher Specification for AT-TLS
 FTPFSPBS - Negotiated Protection Buffer Size
 FTPFSCP - Control Connection Protection Level
 FTPFSDP - Data Connection Protection Level

Retrieval Example

Chart prime shift FTP Server activity for sysid PROD. Use yesterday's data.

```
DATA SELECTED (KEEP=SYSID DAY ZONE HOUR FCFBYTEI FCFBYTEO)
```

```
;
SET &PTCPD..TCPFCF01;
IF SYSID = 'PROD';
IF 9 GE HOUR LE 17; /* SELECT PRIME SHIFT */

PROC CHART DATA=SELECTED;
  VBAR HOUR / SUMVAR=FCFBYTES
  DISCRETE;
TITLE 'DAYS TCPFCF01, PRIME SHIFT IN BYTE COUNT ';
RUN;
```

5.4.5 API Calls for Sockets File (TCPAPI)

The API Calls for Sockets File (TCPAPI) quantifies API calls activity. The API calls are used by a server to provide services to clients. They are also used by clients to establish a communication link with the server.

This file is derived from SMF record types 118 and 119. In SMF record type 118, the API Calls for Sockets record is identified by characters 'INIT' or 'TERM' at offset 21. In SMF record type 119, it is the subtype 2 (TCP connection termination record).

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.4.5.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	TCPLADDR	TCPRADDR	TCPLPORT	
	TCPRPORT	YEAR	MONTH	DAY	HOUR	
	ENDTS					
DAYS	NETWRKID	SYSID	YEAR	MONTH	DAY	
	HOUR					
WEEKS	NETWRKID	SYSID	YEAR	WEEK	ZONE	
MONTHS	NETWRKID	SYSID	YEAR	MONTH	ZONE	
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=DEFAult option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-28. TCPAPI Timespan Granularity Chart

5.4.5.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XD...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	SYSID	- System Identifier
X.....E	TCPLADDR	- Local IP Address (Data Connection)

X.....E TCPLPORT - Local Port Number (Data Connection)
 X.....E TCPRADDR - Remote IP Address (Data Connection)
 X.....E TCPRPORT - Remote Port Number (Data Connection)
 XDWM...E WEEK - Week of Year
 XDWM...E YEAR - Year of Century
 XDWM...E ZONE - Time Zone

Common Data Elements

XDWM...E APIBYTEI - Bytes In
 XDWM...E APIBYTEO - Bytes Out
 XD....E DAYNAME - Name of Day of Week
 XDWM...E DURATION - Recording Interval Time
 XDWM...E ENDTS - End Time Stamp
 XDWM...E MICSVER - CA MICS Version Number
 XDWM...E PRODUCT - Network Product (Source) Name
 XDWM...E STARTTS - Start Time Stamp
 XDWM...E SYSNAME - System Name
 XDWM...E SYSPLEX - Sysplex Name
 X.....E TCPIPTYP - TCP/IP Type
 X.....E TCPSOCID - TCP Socket Resource ID
 X.....E TCPSOCNM - TCP Socket Resource Name
 XDWM...E TCPSSL2 - SSL Protocol V2 Count
 XDWM...E TCPSSL3 - SSL Protocol V3 Count
 X.....E TCPSTACK - TCP/IP Stack Name
 XD....E TCPSTQN - TCP/IP Address Space Name
 XDWM...E TCPTLS1 - TLS Protocol V1 Count
 X.....E TCPUID - User ID
 X.....E TCPVRL - z/OS CS TCP/IP Version/Rel.
 XDWM.. TMOFFSET - Time Offset

Retained Data Elements

X.....E APIAPPL - Target Application Name
 X.....E APIETOD - Connection End Timespan (TOD)
 X.....E APIETS - Connection End Timespan
 X.....E APILMODE - Logmode Name
 X.....E APILU - LU Name
 X.....E APIPOL - Service Policy Name
 X.....E APIPROF - Service Profile Name
 X.....E APIRCODE - Telnet Conn. Term. Reason Code
 XDWM...E APIRTT - Round Trip Time
 XDWM...E APIRTTV - Round Trip Time Variance
 X.....E APISOCST - Socket Status
 X.....E APISTOD - Connection Start Timespan (TOD)
 X.....E APISTS - Connection Start Timespan
 X.....E APITERM - Connection Termination Reason Code
 X.....E APITLSNC - AT-TLS Negotiated Cipher
 X.....E APITLSST - AT-TLS Security Type

X.....E APITLSUI - AT-TLS Partner UserID
X.....E APITOS - Type of Service
X.....E APIUJOB - API User's Job Name

Accumulated Data Elements

XDWM..E APIDACKS - Duplicate ACKs Received Count
XDWM..E APIDRM - Telnet Definite Response Mode Count
XDWM..E APIISEG - Inbound Segment Count
XDWM..E APILNMOD - Telnet Line Mode Count
XDWM..E APIOSEG - Outbound Segment Count
XDWM..E APIPMCT - Telnet Performance Monitored Count
XDWM..E APIRTCNT - Times Retransmission Required
XDWM..E APISWS - Send Window Size
XDWM..E APITLSCH - AT-TLS Connection Handshake Count
XDWM..E APITLSCN - AT-TLS Connection not Secure Count
XDWM..E APITLSCS - AT-TLS Connection Secure Count
XDWM..E APITLSPE - AT-TLS Policy Enabled Count
XDWM..E APITLSPF - AT-TLS Policy Enabled Plus Count
XDWM..E APITLSPG - AT-TLS Policy Not Enabled Count
XDWM..E APITLSPN - AT-TLS no Policy Defined Count
XDWM..E APITLSP0 - AT-TLS Policy Function off Count
XDWM..E APITLSPU - AT-TLS Policy not Known Count
XDWM..E API3270 - Telnet 3270 Mode Count
XDWM..E API3270E - Telnet 3270E Mode Count

Maximum Data Elements

XDWM..E APICWS - Congestion Window Size
XDWM..E APIMSS - Maximum Send Segment Size
XDWM..E APIMXSW - Maximum Send Window Size

5.4.5.3 Usage Considerations

This section identifies special considerations or techniques related to using the TCPAPI File. In addition, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. The API Calls for Sockets File (TCPAPI) is built by selecting data from SMF record type 118 and/or SMF record type 119. The data of type INIT and TERM from SMF type 118 records is selected. An observation of type INIT is matched with the corresponding observation of type TERM before storing it in the STN file. Any observation without an exact match is stored in the API Calls for Sockets Suspend File (TCPSAP). Care must be exercised when combining observations from other TCP files to avoid duplication.

The data from SMF record type 119 subtype 2 (TCP connection termination record) is also used to populate this file. The TCP termination record contains the connection start time and connection end time, thereby eliminating the need to hold session start records in the suspend file to calculate the session duration.

Consult your z/OS CS system programmer to turn off SMF record type 118 and to activate SMF record type 119. This will improve your DAY056 job performance.

2. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.

- o WEEKS should not be used in MONTHS.
3. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
- o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.
4. The following data elements lose significance after summarization has been performed. These data elements should be referenced only when the last observed value in a summarization interval is significant.

TCPRPORT - Remote Port Number (Data Connection)
TCPLPORT - Local Port Number (Data Connection)
TCPRADDR - Remote IP Address (Data Connection)
TCPLADDR - Local IP Address (Data Connection)
TCPSTACK - TCP/IP Stack Name
TCPSOCID - TCP Socket Resource ID
TCPSOCNM - TCP Socket Resource Name
TCPVRRL - z/OS CS TCP/IP Version/Rel.
TCPUID - User ID

Retrieval Example

Chart prime shift API Class for Sockets activity for sysid
PROD. Use yesterday's data.

```
DATA SELECTED (KEEP=SYSID DAY ZONE HOUR APIBYTEI APIBYTE0)
;
SET &PTCPD..TCPAPI01;
IF SYSID = 'PROD';
IF 9 GE HOUR LE 17; /* SELECT PRIME SHIFT */

PROC CHART DATA=SELECTED;
  VBAR HOUR / SUMVAR=APIBYTEI
```

```
DISCRETE;  
TITLE 'DAYS TCPAPI01, PRIME SHIFT IN BYTE COUNT ';  
RUN;
```

5.4.6 FTP Login Failure File (TCPFLF)

The FTP Login Failure File (TCPFLF) contains the activity of all recorded incidents, when FTP user login attempts end in a failure. This activity can be useful to track unauthorized attempts to access the FTP Server.

In SMF record type 119, it is the subtype 72 (FTP Server login failure record).

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.4.6.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	TCPLADDR	TCPLPORT	TCPRADDR	
	TCPRPORT	YEAR	MONTH	DAY	HOUR	
	ENDTS					
DAYS	N/A					
WEEKS	N/A					
MONTHS	N/A					
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=DEfault option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-29. TCPFLF Timespan Granularity Chart

5.4.6.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

X - DETAIL
 D - DAYS
 W - WEEKS
 M - MONTHS
 Y - YEARS
 T - TABLES AREA
 . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

X....E	DAY	- Day of Month
X....E	ENDTS	- End Time Stamp
X....E	HOURL	- Hour of Day
X....E	MONTH	- Month of Year
X....E	NETWRKID	- Network Identifier
X....E	SYSID	- System Identifier

X.....E TCPLADDR - Local IP Address (Data Connection)
X.....E TCPLPORT - Local Port Number (Data Connection)
X.....E TCPRADDR - Remote IP Address (Data Connection)
X.....E TCPRPORT - Remote Port Number (Data Connection)
X.....E WEEK - Week of Year
X.....E YEAR - Year of Century

Common Data Elements

X.....E DAYNAME - Name of Day of Week
X.....E FTPFSCP - Control Connection Protection Level
X.....E FTPFSCS - Cipher Specification
X.....E FTPFSDP - Data Connection Protection Level
X.....E FTPFSLC - Login Method is Certificate Count
X.....E FTPFSLP - Login Method is Password Count
X.....E FTPFSLT - Login Method is Kerberos Count
X.....E FTPFSMA - Security Mechanism AT-TLS Count
X.....E FTPFSMG - Security Mechanism GSSAPI Count
X.....E FTPFSMN - Security Mechanism None Count
X.....E FTPFSMT - Security Mechanism TLS Count
X.....E FTPFSPBS - Negotiated Protection Buffer Size
X.....E MICSVER - CA MICS Version Number
X.....E PRODUCT - Network Product (Source) Name
X.....E SYSNAME - System Name
X.....E SYSPLEX - Sysplex Name
X.....E TCPIPTYP - TCP/IP Type
X.....E TCPSSL2 - SSL Protocol V2 Count
X.....E TCPSSL3 - SSL Protocol V3 Count
X.....E TCPSTACK - TCP/IP Stack Name
X.....E TCPTLS1 - TLS Protocol V1 Count
X.....E TCPUID - User ID
X.....E TCPVRRL - z/OS CS TCP/IP Version/Rel.
X.....E TMOFFSET - Time Offset
X.....E ZONE - Time Zone

Retained Data Elements

X.....E FLFCIDCC - TCP Conn. ID of FTP Control Connection
X.....E FLFFAILR - Login Failure Reason
X.....E FLFSESID - FTP Activity Logging Session id
X.....E FLFUID - Client User ID Received by Server

Accumulated Data Elements

X.....E FLFFSLF - Login Failed Before Login Method Count

5.4.6.3 Usage Considerations

This section identifies special considerations or techniques related to using the TCPFLF File. In addition, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. The FTP Login Failure File (TCPFLF) is built by selecting data from SMF record type 119 subtype 72 (FTP Server login failure record).
2. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, the following fields lose significance and should not be used:
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEKS should not be used in MONTHS.
3. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - Time Offset. TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To

determine the original time the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

4. The following data elements lose significance after summarization has been performed. These data elements should be referenced only when the last observed value in a summarization interval is significant.

TCPRPORT - Remote Port Number (Data Connection)
TCPLPORT - Local Port Number (Data Connection)
TCPRADDR - Remote IP Address (Data Connection)
TCPLADDR - Local IP Address (Data Connection)
TCPSTACK - TCP/IP Stack Name
TCPSOCID - TCP Socket Resource ID
TCPSOCNM - TCP Socket Resource Name
TCPVRRRL - z/OS CS TCP/IP Version/Rel.
TCPUID - User ID
FTPFSCS - Cipher Specification for AT-TLS
FTPFSPBS - Negotiated Protection Buffer Size
FTPFSCP - Control Connection Protection Level
FTPFSDP - Data Connection Protection Level

Retrieval Example

Print the complete listing of today's logon failures. Use yesterday's data.

```
PROC PRINT DATA=&PTCPD..TCPFLF01;  
  BY SYSID;  
  ID SYSID;  
RUN;
```

5.4.7 IP Statistics File (TCPIPX)

The IP Statistics (TCPIPX) file quantifies Internet protocol (IP) statistics. The IP allows to transmit blocks of data (datagram) between source and destination. The source and destination are identified by unique addresses. In addition, IP is capable of fragmenting and reassembling big datagrams that enables it to transmit packets through networks that cannot handle large packets.

The IP protocol is limited in the way it handles packets. There are no built in mechanisms for error checking like reliability, order of data, etc.

This file is derived from IP and/or IPv6 statistics sections of the SMF record type 119 subtype 5 (TCP/IP Statistics record).

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.4.7.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	TCPSTACK	YEAR	MONTH	
	DAY	HOURL	IPVER	ENDTS		
DAYS	NETWRKID	SYSID	TCPSTACK	YEAR	MONTH	
	DAY	HOURL	IPVER			
WEEKS	NETWRKID	SYSID	TCPSTACK	YEAR	WEEK	
	IPVER	ZONE				
MONTHS	NETWRKID	SYSID	TCPSTACK	YEAR	MONTH	
	IPVER	ZONE				
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-25. TCPIPX Timespan Granularity Chart

5.4.7.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XD...E	HOURL	- Hour of Day
XDWM..E	IPVER	- IP Version Type
XD.M..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	SYSID	- System Identifier

XDWM..E TCPSTACK - TCP/IP Stack Name
 XDW...E WEEK - Week of Year
 XDWM..E YEAR - Year of Century
 XDWM..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
 XDWM..E DURATION - Recording Interval Time
 XDWM..E ENDTS - End Time Stamp
 XDWM..E INTERVLS - Number of Recording Intervals
 XDWM.. PRODUCT - Network Product (Source) Name
 XDWM..E STARTTS - Start Time Stamp
 XDWM..E SYSNAME - System Name
 XDWM..E SYSPLEX - Sysplex Name
 X.....E TCPIPTYP - TCP/IP Type
 X.....E TCPUID - User ID
 X.....E TCPVRRL - z/OS CS TCP/IP Version/Rel.
 XDWM.. TMOFFSET - Time Offset

Accumulated Data Elements

XDWM..E IPXCURAR - IPv4 Current Active Reassemblies Count
 XDWM..E IPXDATTf - Attempts to Forward DG Count
 XDWM..E IPXDDE - DG Discarded Count - Address Error
 XDWM..E IPXDDEFF - DG Discarded Count - Fragment Failures
 XDWM..E IPXDDEIS - DG Discarded Count - IP Header Error
 XDWM..E IPXDDELVR - DG Delivered Count
 XDWM..E IPXDDEMS - IPv4 DG Discarded - Memory Shortages
 XDWM..E IPXDDENRA - Out Trans DG Discarded - No Route Avail
 XDWM..E IPXDDEOT - DG Discarded Count - Other Reasons
 XDWM..E IPXDDEOTN - Out Trans DG Discarded - Other Reasons
 XDWM..E IPXDDEUP - DG Discarded Count - Unknown Protocol
 XDWM..E IPXDRA - DG Reassembled Count
 XDWM..E IPXDREC - DG Received Count
 XDWM..E IPXDTRAN - DG Transmitted Count
 XDWM..E IPXFDR - Fragmented DG Received Count
 XDWM..E IPXFRAGG - Fragments Generated Count
 XDWM..E IPXICDL - IPv4 Inbound Calls Count - Device Layer
 XDWM..E IPXRAF - Failed Reassembly Attempts Count
 XDWM..E IPXRDR - DG Received Requiring Assembly Count
 XDWM..E IPXRESTO - Reassembly Timeouts Count
 XDWM..E IPXRFLAG - IPv4 Reassembly Flags
 XDWM..E IPXRFUP - IPv4 Received Frame Unpacking Count
 XDWM..E IPXROUTD - Routing Discards Count
 XDWM..E IPXTDDAE - IPv4 Trans DG Discarded - Async Errors
 XDWM..E IPXTDDMS - IPv4 Trans DG Discarded - Mem Shortages
 XDWM..E IPXTDDSE - IPv4 Trans DG Discarded - Sync Errors

Maximum Data Elements

XDWM..E IPXMXAR - IPv4 Max Active Reassemblies Count

Derived Data Elements

XDWM..E IPXAVDD - Avg DG Delivered Count

XDWM..E IPXAVDR - Avg DG Received Count

XDWM..E IPXAVDT - Avg DG Transmitted Count

5.4.7.3 Usage Considerations

This section identifies special considerations or techniques related to using the TCPIPX file. In addition, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &ddiit, where d is the database identifier, iiii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. The IP Statistics (TCPIPX) file provides information to analyze IPv4 and IPv6 IP protocols in a TCP/IP stack. The data used to create this file comes from SMF record type 119 subtype 5. This subtype provides data for six different protocols, IPv4 IP, TCP, UDP, IPv4 ICMP, IPv6 IP, and IPv6 ICMP. The TCPIPX file is specifically built from data found in IPv4 IP and IPv6 IP statistics sections.
2. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEKS should not be used in MONTHS.
3. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - TIME OFFSET applied to the data in the file.

The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

4. The following data elements lose significance after summarization has been performed. These data elements should be referenced only when the last observed value in a summarization interval is significant.

TCPIPTYP - TCP/IP Type
TCPSOCID - TCP Socket Resource ID
TCPVRRRL - z/OS CS TCP/IP Version/Rel.
TCPUID - User ID

Retrieval Example

Chart prime shift IP Protocol activity for Sysid PROD. Use yesterday's data.

```
DATA SELECTED (KEEP=SYSID IPVER DAY ZONE HOUR IPXDREC );
  SET &TCPD..TCPIPX01;
  IF SYSID = 'PROD';
  IF 9 GE HOUR LE 17; /* SELECT PRIME SHIFT */
RUN;

PROC SORT DATA=SELECTED;
  BY SYSID IPVER;

PROC CHART DATA=SELECTED;
  BY SYSID IPVER;
  VBAR HOUR / SUBGROUP=IPVER SUMVAR=IPXDREC
  DISCRETE;
TITLE1 'DAYS TCPIPX01, PRIME SHIFT IN DATAGRAMS RECEIVED';
RUN;
```

5.4.8 ICMP Statistics File (TCPICX)

The ICMP Statistics (TCPICX) file quantifies ICMP protocol statistics. The Internet Control Message Protocol (ICMP) allows communication between destination host and the source host to report errors in processing the datagrams. ICMP is an integral part of IP.

ICMP protocol is used in situations like failure of datagram to reach its destination, lack of buffering capacity in a gateway to forward datagrams, and ability of a gateway to forward the datagram on a shorter route.

This file is derived from ICMP and/or IPv6 ICMP statistics sections of the SMF record type 119 subtype 5 (TCP/IP Statistics record).

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.4.8.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	TCPSTACK	YEAR	MONTH	
	DAY	HOURL	IPVER	ENDTS		
DAYS	NETWRKID	SYSID	TCPSTACK	YEAR	MONTH	
	DAY	HOURL	IPVER			
WEEKS	NETWRKID	SYSID	TCPSTACK	YEAR	WEEK	
	IPVER	ZONE				
MONTHS	NETWRKID	SYSID	TCPSTACK	YEAR	MONTH	
	IPVER	ZONE				
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-26. TCPICX Timespan Granularity Chart

5.4.8.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XD...E	HOURL	- Hour of Day
XDWM..E	IPVER	- IP Version Type
XD.M..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier

XDWM..E SYSID - System Identifier
 XDWM..E TCPSTACK - TCP/IP Stack Name
 XDW...E WEEK - Week of Year
 XDWM..E YEAR - Year of Century
 XDWM..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
 XDWM..E DURATION - Recording Interval Time
 XDWM..E ENDTS - End Time Stamp
 XDWM..E INTERVLS - Number of Recording Intervals
 XDWM.. PRODUCT - Network Product (Source) Name
 XDWM..E STARTTS - Start Time Stamp
 XDWM..E SYSNAME - System Name
 XDWM..E SYSPLEX - Sysplex Name
 X.....E TCPIPTYP - TCP/IP Type
 X.....E TCPUID - User ID
 X.....E TCPVRRL - z/OS CS TCP/IP Version/Rel.
 XDWM.. TMOFFSET - Time Offset

Accumulated Data Elements

XDWM..E ICXIIAMM - IPv4 Inbound ICMP Addr Mask Rqst Msgs
 XDWM..E ICXIARM - IPv4 Inbound ICMP Addr Mask Reply Msgs
 XDWM..E ICXIICAM - IPv6 Inbound ICMP Admin Prohibit Msgs
 XDWM..E ICXIICBM - IPv6 Inbound ICMP Packet Too Big Msgs
 XDWM..E ICXIICEM - Inbound ICMP Error Msgs
 XDWM..E ICXIICM - Inbound ICMP Msgs
 XDWM..E ICXIICPM - Inbound ICMP Parameter Problem Msgs
 XDWM..E ICXIICQM - IPv4 Inbound ICMP Source Quench Msgs
 XDWM..E ICXIICRM - Inbound ICMP Redirect Msgs
 XDWM..E ICXIICUM - Inbound ICMP Dest Unreachable Msgs
 XDWM..E ICXIICXM - Inbound ICMP Time Exceeded Msgs
 XDWM..E ICXIICYM - Inbound ICMP Echo Rqst Msgs
 XDWM..E ICXIICZM - Inbound ICMP Echo Reply Msgs
 XDWM..E ICXIILQM - IPv6 Inbound ICMP MLDM Query Msgs
 XDWM..E ICXIILRD - IPv6 Inbound ICMP MLDM Reductn Msgs
 XDWM..E ICXIILRM - IPv6 Inbound ICMP MLDM Reply Msgs
 XDWM..E ICXIINAM - IPv6 Inbound ICMP Neighbr Advrtise Msgs
 XDWM..E ICXIINSM - IPv6 Inbound ICMP Neighbr Solicit Msgs
 XDWM..E ICXIIRAM - IPv6 Inbound ICMP Router Advrtise Msgs
 XDWM..E ICXIIRSM - IPv6 Inbound ICMP Router Solicit Msgs
 XDWM..E ICXIIRTM - IPv4 Inbound ICMP Timestamp Reply Msgs
 XDWM..E ICXIITRM - IPv4 Inbound ICMP Timestamp Rqst Msgs
 XDWM..E ICXOIAMM - IPv4 Outbound ICMP Addr Mask Rqst Msgs
 XDWM..E ICXOARM - IPv4 Outbound ICMP Addr Mask Reply Msgs
 XDWM..E ICXOICAM - IPv6 Outbound ICMP Admin Prohibit Msgs
 XDWM..E ICXOICBM - IPv6 Outbound ICMP Packet Too Big Msgs

XDWM..E ICX0ICEM - Outbound ICMP Error Msgs
XDWM..E ICX0ICM - Outbound ICMP Msgs
XDWM..E ICX0ICPM - Outbound ICMP Parameter Problem Msgs
XDWM..E ICX0ICQM - IPv4 Outbound ICMP Source Quench Msgs
XDWM..E ICX0ICRM - Outbound ICMP Redirect Msgs
XDWM..E ICX0ICUM - Outbound ICMP Dest Unreachable Msgs
XDWM..E ICX0ICXM - Outbound ICMP Time Exceeded Msgs
XDWM..E ICX0ICYM - Outbound ICMP Echo Rqst Msgs
XDWM..E ICX0ICZM - Outbound ICMP Echo Reply Msgs
XDWM..E ICX0ILQM - IPv6 Outbound ICMP MLDM Query Msgs
XDWM..E ICX0ILRD - IPv6 Outbound ICMP MLDM Reduction Msgs
XDWM..E ICX0ILRM - IPv6 Outbound ICMP MLDM Reply Msgs
XDWM..E ICX0INAM - IPv6 Outbound ICMP Neighbor Advrtise Msgs
XDWM..E ICX0INSM - IPv6 Outbound ICMP Neighbor Solicit Msgs
XDWM..E ICX0IRAM - IPv6 Outbound ICMP Router Advrtise Msgs
XDWM..E ICX0IRSM - IPv6 Outbound ICMP Router Solicit Msgs
XDWM..E ICX0IRTM - IPv4 Outbound ICMP Timestamp Reply Msgs
XDWM..E ICX0ITRM - IPv4 Outbound ICMP Timestamp Rqst Msgs

Maximum Data Elements

XDWM..E ICXMXIIM - Max Inbound ICMP Msgs
XDWM..E ICXMXOIM - Max Outbound ICMP Msgs

Derived Data Elements

XDWM..E ICXAVIIE - Avg Inbound ICMP Error Msgs
XDWM..E ICXAVOIE - Avg Outbound ICMP Error Msgs
XDWM..E ICXPCIIE - Pct Inbound ICMP Error Msgs
XDWM..E ICXPCOIE - Pct Outbound ICMP Error Msgs

5.4.8.3 Usage Considerations

This section identifies special considerations or techniques related to using the TCPICX file. In addition, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. The ICMP Statistics (TCPICX) file provides information to analyze IPv4 and IPv6 ICMP protocols in a TCP/IP stack. The data used to create this file comes from SMF record type 119 subtype 5. This subtype provides data for six different protocols, IPv4 IP, TCP, UDP, IPv4 ICMP, IPv6 IP, and IPv6 ICMP. The TCPICX file is specifically built from data found in IPv4 IP and IPv6 ICMP statistics sections.
2. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEKS should not be used in MONTHS.
3. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique

NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

4. The following data elements lose significance after summarization has been performed. These data elements should be referenced only when the last observed value in a summarization interval is significant.

TCPIPTYP - TCP/IP Type
TCPSOCID - TCP Socket Resource ID
TCPVRRLL - z/OS CS TCP/IP Version/Rel.
TCPUID - User ID

Retrieval Example

Chart prime shift ICMP Protocol activity for Sysid PROD. Use yesterday's data.

```
DATA SELECTED (KEEP=SYSID IPVER DAY ZONE HOUR ICXIICM );
  SET &TCPD..TCPICX01;
  IF SYSID = 'PROD';
  IF 9 GE HOUR LE 17; /* SELECT PRIME SHIFT */
RUN;

PROC SORT DATA=SELECTED;
  BY SYSID IPVER;

PROC CHART DATA=SELECTED;
  BY SYSID IPVER;
  VBAR HOUR / SUBGROUP=IPVER SUMVAR=ICXIICM
  DISCRETE;
TITLE1 'DAYS TCPICX01, PRIME SHIFT IN DATAGRAMS RECEIVED';
RUN;
```

5.4.9 TCP Statistics File (TCPTCI)

The TCP Statistics (TCPTCI) file quantifies Transmission Control Protocol (TCP) statistics. The TCP allows to transmit variable length segments enclosed in internet datagram envelopes. The datagrams contain information about source and destination TCPs in different networks. Moreover, the internet protocol also provides means to deal with fragmentation and reassembly of TCP segmentation.

The TCP is a highly reliable host-to-host protocol providing connectivity between hosts in packet-switched communication network, and interconnected systems of such networks.

This file is derived from TCP statistics section of the SMF record type 119 subtype 5 (TCP/IP Statistics record).

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.4.9.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	TCPSTACK	YEAR	MONTH	
	DAY	HOUR	ENDTS			
DAYS	NETWRKID	SYSID	TCPSTACK	YEAR	MONTH	
	DAY	HOUR				
WEEKS	NETWRKID	SYSID	TCPSTACK	YEAR	WEEK	
	ZONE					
MONTHS	NETWRKID	SYSID	TCPSTACK	YEAR	MONTH	
	ZONE					
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-27. TCPTCI Timespan Granularity Chart

5.4.9.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XD...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	SYSID	- System Identifier
XDWM..E	TCPSTACK	- TCP/IP Stack Name

XDW...E WEEK - Week of Year
 XDW..E YEAR - Year of Century
 XDW..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
 XDW..E DURATION - Recording Interval Time
 XDW..E ENDTS - End Time Stamp
 XDW..E INTERVLS - Number of Recording Intervals
 XDW.. PRODUCT - Network Product (Source) Name
 XDW..E STARTTS - Start Time Stamp
 XDW..E SYSNAME - System Name
 XDW..E SYSPLEX - Sysplex Name
 X.....E TCPIPTYP - TCP/IP Type
 X.....E TCPUID - User ID
 X.....E TCPVRRL - z/OS CS TCP/IP Version/Rel.
 XDW.. TMOFFSET - Time Offset

Accumulated Data Elements

XDW..E TCIAOCON - Active Open Connection Count
 XDW..E TCICDSR - Rec Complete Dup Segments Count
 XDW..E TCICONAD - TCP Conn Attempts Discarded Count
 XDW..E TCICONCL - TCP Connections Closed Count
 XDW..E TCICONDF - TCP Conn Dropped - FINWAIT2 Count
 XDW..E TCICONDK - TCP Conn Dropped - KeepAlive Count
 XDW..E TCICONDP - TCP Conn Dropped - Probes Count
 XDW..E TCICONDR - TCP Conn Dropped - Retrans Count
 XDW..E TCICSRWC - Complete Segments Rec - AWC Count
 XDW..E TCICURES - Current Establishments Count
 XDW..E TCIDACKR - Duplicate ACKs Received Count
 XDW..E TCIFOCON - Open Connection Failures Count
 XDW..E TCIHDRPA - Header Predictions Ok for ACK Count
 XDW..E TCIHDRPD - Header Predictions Ok for Data Count
 XDW..E TCIIERR - Input Errors Count
 XDW..E TCIISEG - Input TCP Segments Count
 XDW..E TCIMTUBL - Path MTUs Beyond Retrans Lim Count
 XDW..E TCIOSEG - Output TCP Segments Count
 XDW..E TCIPDSR - Rec Partial Dup Segments Count
 XDW..E TCIPOCON - Passive Open Connection Count
 XDW..E TCIPSRWC - Partial Segments Rec - AWC Count
 XDW..E TCIRECON - Connection Resets Count
 XDW..E TCIRESEG - Retransmitted Segments Count
 XDW..E TCIRESET - Resets Count
 XDW..E TCIRMTU - Retrans Path MTU Disc Packet Count
 XDW..E TCIRPDBC - Rec Packets Discarded - Bad Chksum Count
 XDW..E TCIRPDBH - Rec Packets Discarded - Bad HdrLen Count
 XDW..E TCIRPDID - Rec Packets Discarded - Insf Data Count

XDM..E TCIRPDOT - Rec Packets Discarded - Old TS Count
XDM..E TCIRTALG - Retransmission Algorithm
XDM..E TCIRTTT - Retransmitted Timeouts Count
XDM..E TCIRWP - Received Window Probes Count
XDM..E TCIRWU - Received Window Updates Count
XDM..E TCISRACC - Segment Rec - After Conn Close Count
XDM..E TCISROO - Out of Order Segments Rec Count
XDM..E TCITCONR - TCP Timewait Conn Refused Count
XDM..E TCITDACK - Transmitted Delayed ACKs Count
XDM..E TCITKAP - Transmitted KeepAlive Probes Count
XDM..E TCITWP - Transmitted Window Probes Count
XDM..E TCITWU - Transmitted Window Updates Count

Minimum Data Elements

XDM..E TCIMNRT - Min Retransmission Time

Maximum Data Elements

XDM..E TCIMXRT - Max Retransmission Time
XDM..E TCIMXTC - Max TCP Connections Count

5.4.9.3 Usage Considerations

This section identifies special considerations or techniques related to using the TCPTCI file. In addition, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. The TCP Statistics (TCPTCI) file provides information to analyze TCP protocol in a TCP/IP stack. The data used to create this file comes from SMF record type 119 subtype 5. This subtype provides data for six different protocols, IPv4 IP, TCP, UDP, IPv4 ICMP, IPv6 IP, and IPv6 ICMP. The TCPTCI file is specifically built from data found in TCP statistics section.
2. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEKS should not be used in MONTHS.
3. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to

adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

4. The following data elements lose significance after summarization has been performed. These data elements should be referenced only when the last observed value in a summarization interval is significant.

TCPIPTYP - TCP/IP Type
TCPSOCID - TCP Socket Resource ID
TCPVRRL - z/OS CS TCP/IP Version/Rel.
TCPUID - User ID

Retrieval Example

Chart prime shift TCP Protocol activity for Sysid PROD. Use yesterday's data.

```
DATA SELECTED (KEEP=SYSID TCPSTACK DAY ZONE HOUR TCIDACKR);  
  SET &TCPD..TCPTCI01;  
  IF SYSID = 'PROD';  
  IF 9 GE HOUR LE 17; /* SELECT PRIME SHIFT */  
RUN;  
  
PROC CHART DATA=SELECTED;  
  BY SYSID TCPSTACK;  
  VBAR HOUR / SUMVAR=TCIDACKR SUBGROUP=TCPSTACK  
  DISCRETE;  
  TITLE1 'DAYS TCPTCI01, PRIME SHIFT IN DATAGRAMS RECEIVED';  
RUN;
```

5.4.10 UDP Statistics File (TCPUDI)

The UDP Statistics (TCPUDI) file quantifies User Datagram Protocol (UDP) statistics. The UDP is defined to make available a datagram mode of packet-switched computer communication in the environment of an interconnected set of computer networks. It assumes that IP is used as the underlying protocol.

UDP provides a way for application programs to send message to other programs with a minimum of protocol mechanism. It is transaction oriented, delivery and duplicate protection are not guaranteed. Programs requiring reliable delivery of data should use TCP.

This file is derived from UDP statistics section of the SMF record type 119 subtype 5 (TCP/IP Statistics record).

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.4.10.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	TCPSTACK	YEAR	MONTH	
	DAY	HOURL	ENDTS			
DAYS	NETWRKID	SYSID	TCPSTACK	YEAR	MONTH	
	DAY	HOURL				
WEEKS	NETWRKID	SYSID	TCPSTACK	YEAR	WEEK	
	ZONE					
MONTHS	NETWRKID	SYSID	TCPSTACK	YEAR	MONTH	
	ZONE					
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-28. TCPUDI Timespan Granularity Chart

5.4.10.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XD...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	SYSID	- System Identifier
XDWM..E	TCPSTACK	- TCP/IP Stack Name

XDW...E WEEK - Week of Year
XDWM..E YEAR - Year of Century
XDWM..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
XDWM..E DURATION - Recording Interval Time
XDWM..E ENDTS - End Time Stamp
XDWM..E INTERVLS - Number of Recording Intervals
XDWM.. PRODUCT - Network Product (Source) Name
XDWM..E STARTTS - Start Time Stamp
XDWM..E SYSNAME - System Name
XDWM..E SYSPLEX - Sysplex Name
X.....E TCPIPTYP - TCP/IP Type
X.....E TCPUID - User ID
X.....E TCPVRRL - z/OS CS TCP/IP Version/Rel.
XDWM.. TMOFFSET - Time Offset

Accumulated Data Elements

XDWM..E UDIDNOTR - Other UDP Datagrams Not Rec Count
XDWM..E UDIDREC - UDP Datagrams Received Count
XDWM..E UDIDRNOP - UDP Datagrams Rec - No Port Count
XDWM..E UDIDSENT - UDP Datagrams Sent Count

Derived Data Elements

XDWM..E UDIAVDR - Avg UDP Datagrams Received Count
XDWM..E UDIAVDS - Avg UDP Datagrams Sent Count

5.4.10.3 Usage Considerations

This section identifies special considerations or techniques related to using the TCPUDI file. In addition, several retrieval examples are provided to facilitate the use of this file.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &diit, where d is the database identifier, ii is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. The UDP Statistics (TCPUDI) file provides information to analyze UDP protocol in a TCP/IP stack. The data used to create this file comes from SMF record type 119 subtype 5. This subtype provides data for six different protocols, IPv4 IP, TCP, UDP, IPv4 ICMP, IPv6 IP, and IPv6 ICMP. The TCPUDI file is specifically built from data found in UDP statistics section.
2. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEKS should not be used in MONTHS.
3. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to

adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

4. The following data elements lose significance after summarization has been performed. These data elements should be referenced only when the last observed value in a summarization interval is significant.

TCPIPTYP - TCP/IP Type
 TCPSOCID - TCP Socket Resource ID
 TCPVRR - z/OS CS TCP/IP Version/Rel.
 TCPUID - User ID

Retrieval Example

Chart prime shift UDP Protocol activity for Sysid PROD. Use yesterday's data.

```
DATA SELECTED (KEEP=SYSID TCPSTACK DAY ZONE HOUR UDIDREC);
  SET &TCPD..TCPUDI01;
  IF SYSID = 'PROD';
  IF 9 GE HOUR LE 17; /* SELECT PRIME SHIFT */
RUN;

PROC CHART DATA=SELECTED;
  BY SYSID TCPSTACK;
  VBAR HOUR / SUMVAR=UDIDREC SUBGROUP=TCPSTACK
  DISCRETE;
TITLE1 'DAYS TCPUDI01, PRIME SHIFT IN DATAGRAMS RECEIVED';
RUN;
```

5.4.11 Storage Statistics File (TCPSTG)

The Storage Statistics (TCPSTG) file quantifies Extended Common Service Area (ECSA) statistics. The ECSA is allocated using ECSALimit parameter of GlobalConfig command where as authorized private storage is allocated using POOLSIZE parameter.

This file is derived from storage statistics section of the SMF record type 119 subtype 5 (TCP/IP Statistics record).

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.4.11.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	TCPSTACK	YEAR	MONTH	
	DAY	HOUR	ENDTS			
DAYS	NETWRKID	SYSID	TCPSTACK	YEAR	MONTH	
	DAY	HOUR				
WEEKS	NETWRKID	SYSID	TCPSTACK	YEAR	WEEK	
	ZONE					
MONTHS	NETWRKID	SYSID	TCPSTACK	YEAR	MONTH	
	ZONE					
YEARS	N/A					
TABLES	N/A					

Generation Date: Tue, May 12, 2009

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-29. TCPSTG Timespan Granularity Chart

5.4.11.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Tue, May 12, 2009

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XD...E	HOURL	- Hour of Day
XD.M..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier
XDWM..E	SYSID	- System Identifier
XDWM..E	TCPSTACK	- TCP/IP Stack Name

XDW...E WEEK - Week of Year
XDWM..E YEAR - Year of Century
XDWM..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
XDWM..E DURATION - Recording Interval Time
XDWM..E ENDTS - End Time Stamp
XDWM..E INTERVLS - Number of Recording Intervals
XDWM.. PRODUCT - Network Product (Source) Name
XDWM..E STARTTS - Start Time Stamp
XDWM..E SYSNAME - System Name
XDWM..E SYSPLEX - Sysplex Name
X.....E TCPIPTYP - TCP/IP Type
X.....E TCPUID - User ID
X.....E TCPVRL - z/OS CS TCP/IP Version/Rel.
XDWM.. TMOFFSET - Time Offset

Accumulated Data Elements

XDWM..E STGAPSA - Auth Private Storage Bytes Allocated
XDWM..E STGAPSF - Auth Private Storage Bytes Free
XDWM..E STGAPSU - Auth Private Storage Bytes Used
XDWM..E STGECSAA - ECSA Storage Bytes Allocated
XDWM..E STGECSAF - ECSA Storage Bytes Free
XDWM..E STGECSAU - ECSA Storage Bytes Used

Minimum Data Elements

XDWM..E STGMNAPF - Min Auth Private Storage Bytes Free
XDWM..E STGMNECF - Min ECSA Storage Bytes Free

Maximum Data Elements

XDWM..E STGMXAPF - Max Auth Private Storage Bytes Free
XDWM..E STGMXECF - Max ECSA Storage Bytes Free

5.4.11.3 Usage Considerations

This section identifies special considerations or techniques related to using the TCPSTG file and provides a retrieval example.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &ddiit, where d is the database identifier, iit is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. The Storage Statistics (TCPSTG) file provides information to analyze ECSA and authorized private storage used by the TCP/IP address space. Shortages of storage available for TCP/IP address space during peak times can be critical to business.
2. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEKS should not be used in MONTHS.
3. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is

brought together in the CA MICS database. To determine the original time at which the data was recorded, subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

4. The following data elements lose significance after summarization has been performed. These data elements should be referenced only when the last observed value in a summarization interval is significant.

TCPIPTYP - TCP/IP Type
TCPSOCID - TCP Socket Resource ID
TCPVRRL - z/OS CS TCP/IP Version/Rel.
TCPUID - User ID

Retrieval Example

Chart prime shift storage used for sysid PROD. Use yesterday's data.

```
DATA SELECTED (KEEP=SYSID TCPSTACK DAY ZONE HOUR UDIDREC);
  SET &TCPD..TCPSTG01;
  IF SYSID = 'PROD';
  IF 9 GE HOUR LE 17; /* SELECT PRIME SHIFT */
RUN;

PROC CHART DATA=SELECTED;
  BY SYSID TCPSTACK;
  VBAR HOUR / SUMVAR=STGECSAU SUBGROUP=TCPSTACK
  DISCRETE;
TITLE1 'DAYS TCPSTG01, PRIME SHIFT - TCP/IP STORAGE USED';
RUN;
```

5.4.12 Interface Statistics File (TCPIFS)

The Interface Statistics (TCPIFS) file quantifies statistics for user-defined interfaces (Links or Interfaces). The LINK statement defines the IPv4 interface and INTERFACE statement is used to define IPv6 interfaces.

This file is derived from interface statistics section of the SMF record type 119 subtype 6 (TCP/IP Interface Statistics record). One interface section is recorded for each defined link or interface that contributes to one observation in the TCPIFS file.

The following sections describe the file's organization, list the data elements maintained, and provide usage hints.

- 1 - File Organization
- 2 - Data Elements List
- 3 - Usage Considerations

5.4.12.1 File Organization

The table below identifies data elements by which the file is sequenced and summarized in each timespan. N/A indicates that the file is not supported in a timespan. At the DETAIL level, data is sequenced but not summarized.

NOTE: The timespans in which a file is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

Timespan	Level of Data Granularity					
DETAIL	NETWRKID	SYSID	TCPSTACK	IFSNAME	YEAR	
	MONTH	DAY	HOUR	ENDTS		
DAYS	NETWRKID	SYSID	TCPSTACK	IFSNAME	YEAR	
	MONTH	DAY	HOUR			
WEEKS	NETWRKID	SYSID	TCPSTACK	IFSNAME	YEAR	
	WEEK	ZONE				
MONTHS	NETWRKID	SYSID	TCPSTACK	IFSNAME	YEAR	
	MONTH	ZONE				
YEARS	N/A					
TABLES	N/A					

Generation Date: Wed, Apr 7, 2010

NOTE: This file was generated with ESSENTIAL=ALL option in effect. All data elements defined in the file are generated.

NOTE: This file was generated with DERIVED=Default option in effect. Whether data elements are kept on the file on auxiliary storage or not is controlled by the complex definition of the DERIVED option.

Figure 5-30. TCPIFS Timespan Granularity Chart

5.4.12.2 Data Elements List

The table below identifies data elements contained in this file. The entries for each data element are:

TIMESPAN: Defines the timespans in which the data element is supported. The timespans are indicated by the letters "XDWMYT" as follows:

- X - DETAIL
- D - DAYS
- W - WEEKS
- M - MONTHS
- Y - YEARS
- T - TABLES AREA
- . - File is not supported

The timespan field also indicates Essential Elements with the letter E, if applicable.

DATA ELEMENT: The data element name.

DATA ELEMENT DESCRIPTION: The data element's long name.

The timespans in which a data element is supported are defined by each installation when CA MICS is installed. Therefore, this table has been generated as part of the installation process to accurately reflect the CA MICS system at your installation.

GENERATION DATE: Wed, Apr 7, 2010

Note: Essential data elements are identified by an "E" under the Timespan asterisk (*) column.

Time- Span *	Data Element	Data Element Description (LABEL)
-----	-----	-----

Sequence/Summary Data Elements

XD...E	DAY	- Day of Month
XD...E	HOURL	- Hour of Day
XDWM..E	IFSNAME	- Link or Interface Name
XD.M..E	MONTH	- Month of Year
XDWM..E	NETWRKID	- Network Identifier

XDWM..E SYSID - System Identifier
 XDWM..E TCPSTACK - TCP/IP Stack Name
 XDW...E WEEK - Week of Year
 XDWM..E YEAR - Year of Century
 XDWM..E ZONE - Time Zone

Common Data Elements

XD....E DAYNAME - Name of Day of Week
 XDWM..E DURATION - Recording Interval Time
 XDWM..E ENDTS - End Time Stamp
 XDWM..E INTERVLS - Number of Recording Intervals
 XDWM.. PRODUCT - Network Product (Source) Name
 XDWM..E STARTTS - Start Time Stamp
 XDWM..E SYSNAME - System Name
 XDWM..E SYSPLEX - Sysplex Name
 X.....E TCPIPTYP - TCP/IP Type
 X.....E TCPUID - User ID
 X.....E TCPVRRL - z/OS CS TCP/IP Version/Rel.
 XDWM.. TMOFFSET - Time Offset

Retained Data Elements

X.....E IFSDESC - Interface Description
 X.....E IFSDEVN - Device Name
 X.....E IFSHADDR - Interface HOME Address
 X.....E IFSHPED - HSpeed (Mbits/Sec)
 X.....E IFSMTUSZ - Maximum Transmission Unit (MTU) Size
 X.....E IFSQLEN - Current Output Queue Length
 X.....E IFSSPEED - Speed (Bits/Sec)

Accumulated Data Elements

XDWM..E IFSIBPKT - Inbound Broadcast Packet Count
 XDWM..E IFSIBYCT - Inbound Bytes Count
 XDWM..E IFSIDPKT - Inbound Discarded Packets Count
 XDWM..E IFSIEPKT - Inbound Packets in Error Count
 XDWM..E IFSIMPKT - Inbound Multicast Packets Count
 XDWM..E IFSIPPKT - Inbound Packets - Unknown Protocol Count
 XDWM..E IFSIUPKT - Inbound Unicast Packets Count
 XDWM..E IFSOBPKT - Outbound Broadcast Packet Count
 XDWM..E IFSOBYCT - Outbound Bytes Count
 XDWM..E IFSODPKT - Outbound Discarded Packets Count
 XDWM..E IFSOEPKT - Outbound Packets in Error Count
 XDWM..E IFSOMPKT - Outbound Multicast Packets Count
 XDWM..E IFSOUPKT - Outbound Unicast Packets Count

Derived Data Elements

XDWM..E IFSPSIBC - Inbound Bytes Count per Second
XDWM..E IFSPSOBC - Outbound Bytes Count per Second

5.4.12.3 Usage Considerations

This section identifies special considerations or techniques related to using the TCPIFS file and provides a retrieval example.

In the examples, a SAS macro variable is used to specify the DDname part of the CA MICS file name. These macro variables are a standard part of CA MICS and are available for all files. The macro variable name has the form &ddiit, where d is the database identifier, iit is the information area name, and t is the timespan. For the examples, a database identifier of P is used. The identifier is installation dependent, so you should find out what the identifiers are at your installation.

Special Considerations/Techniques

1. The Interface Statistics (TCPIFS) file provides information to analyze interface statistics for user-defined interfaces (Links or Interfaces). The SMF data provides the statistics for non-VIPA and non-loopback interfaces only.
2. Care must be exercised in using the special date and time data elements contained in each CA MICS file. As file granularity increases in higher timespans, certain fields lose significance and should not be used in those cases.
 - o HOUR should not be used in MONTHS.
 - o DAY and DAYNAME should not be used in WEEKS or MONTHS.
 - o WEEKS should not be used in MONTHS.
3. The following data elements are user-defined. The value in each depends on user-selected options or user-supplied SAS code:
 - o NETWRKID - Network Identifier. A one to eight-character descriptive name for each network represented in the data. NETWRKID is set in the Network Identifier Exit Routine, SNTNIDRT, discussed in Chapter 7.
 - o TMOFFSET - TIME OFFSET applied to the data in the file. The user can associate a TIME OFFSET with each unique NETWRKID/SYSID combination. This offset is used to adjust data times when data from multiple time zones is brought together in the CA MICS database. To determine the original time at which the data was recorded,

subtract TMOFFSET from the value. TIME OFFSET is assigned in the SNTOPS member of prefix.MICS.PARMS, discussed in Chapter 7.

4. The following data elements lose significance after summarization has been performed. These data elements should be referenced only when the last observed value in a summarization interval is significant.

TCPIPTYP - TCP/IP Type
TCPVRRRL - z/OS CS TCP/IP Version/Rel.
TCPUID - User ID

Retrieval Example

Chart prime shift number of inbound packet errors for SYSID PROD. Use yesterday's data.

```
DATA SELECTED (KEEP=SYSID TCPSTACK DAY ZONE HOUR);
  SET &TCPD..TCPIFS01;
  IF SYSID = 'PROD';
  IF 9 GE HOUR LE 17; /* SELECT PRIME SHIFT */
RUN;

PROC CHART DATA=SELECTED;
  BY SYSID TCPSTACK;
  VBAR HOUR / SUMVAR=IFSIEPKT SUBGROUP=TCPSTACK
  DISCRETE;
  TITLE1 'DAYS TCPIFS01, PRIME SHIFT - INBOUND PACKET
  ERRORS';
RUN;
```

Chapter 6: DATA SOURCES

The CA MICS Network Analyzer Option supports the following data sources:

- o CA NetSpy Network Performance
- o CA NetMaster Network Management for TCP/IP release 11.0 (release 11.5 will no longer generate these records.)
- o CA NetMaster Network Management for SNA (Network Tracking System (NTS))
- o CA NetMaster Network Management for SNA (Network Error Warning System (NEWS))
- o Tivoli NetView Performance Monitor (NPM)
- o Tivoli NetView Session Monitor (NLDM)
- o Tivoli NetView Hardware Monitor (NPDA)
- o IBM TCP/IP for z/OS

Note: CA NetSpy Network Performance is integrated with CA NetMaster NM for TCP/IP. If you are a current user of CA NetMaster, you may already be generating or can generate SMF type records that are identical to records generated by CA NetSpy. The SMF data generated by either CA NetMaster or CA NetSpy will be processed and stored by the CA MICS Network Analyzer. Therefore, all references to CA NetSpy also apply to CA NetMaster Network Management for TCP/IP.

This section contains the following topics:

- [6.1 Data Sources Overview](#) (see page 964)
- [6.2 Processing Network Monitor Data From VM Hosts](#) (see page 1002)
- [6.3 Correlating Data Sources](#) (see page 1025)
- [6.4 Exceptions and NPM Network Parameters](#) (see page 1056)
- [6.5 NPA to File Conversion Utility](#) (see page 1061)
- [6.6 Basic Network Accounting](#) (see page 1062)
- [6.7 Identifying Local Vs. Remote Sessions \(ffflDEV\)](#) (see page 1070)
- [6.8 Multiple Session Manager Considerations](#) (see page 1071)
- [6.9 Processing Network Monitor Data From VM Hosts](#) (see page 1075)
- [6.10 CA MICS and CA SMF Director Interface](#) (see page 1076)

6.1 Data Sources Overview

You must coordinate with your network administrator to ensure that data is collected for at least one of the data sources supported by the CA MICS Network Analyzer.

More information about each data source's requirements is found in the following sections:

- 1 - NetView Performance Monitor (NPM)
- 2 - NetView Session Monitor/NLDM
- 3 - NetView Hardware Monitor/NPDA
- 4 - CA NetSpy
- 5 - CA NetMaster Network Tracking System (NTS)
- 6 - CA NetMaster Network Error Warning System (NEWS)
- 7 - CA NetMaster for TCP/IP
- 8 - IBM TCP/IP for z/OS

6.1.1 NetView Performance Monitor (NPM)

Tivoli NetView Performance Monitor (NPM) is an operational performance tool used to monitor and manage day-to-day network operations. Its data collection subsystem has the following collector functions:

- o Network Collector Function - records volume, performance, and reliability data as collected in the network control program (NCP).
- o Session Collector Function - gathers response time and loads data in the host computer.
- o Network Session Accounting - gathers accounting data (connect time and traffic statistics for terminal sessions) from the NCP NPALU (Network Performance Analysis Logical Unit).
- o Network Gateway Accounting - gathers accounting data (connect time and traffic statistics for cross-network sessions) from the NCP NPALU (Network Performance Analysis Logical Unit).

The CA MICS Network Analyzer Option supports the following data, discussed in the Tivoli NetView Performance Monitor documentation, SMF and NPM Log Records section:

+-----+-----+-----+-----+-----+-----+					
IBM Keyword					
Description		Hex Value			
=====		=====			
NETWORK					
NCP Interval		10			
Line Interval		11			
PU Interval		12			
LU Interval		13			
Network Monitor Exception		18			
Network Monitor Resolution		19			
NTRI Logical Link		70			
NTRI Physical Link		71			
X.25 (NPSI, XI) Link Interval		74			
X.25 (NPSI, XI) PU Interval		75			
NPSI VC Interval		77			
Frame Relay Physical Link		82			
Frame Relay Logical Link		83			
Frame Relay Physical Station		84			
Frame Relay (LMI) PU		85			

	ODLC LAN Physical Link		A0	
	ODLC LAN Station PU		A1	
	SESSION			
	LU Detail		20	
	NSA			
	NSA Session Start		50	
	NSA Session Stop		51	
	NSA Interval		52	
	NGA Session Start		60	
	NGA Session Stop		61	
	NGA Interval		62	
	VTAM			
	VTAM Buffer Data		D7	
	VTAM CSM Data		DC	
	VTAM Global Data		D6	
+-----+				

Using NPM Data from VM Systems

When NPM runs on VM systems, a log record that is equivalent to SMF type 28 data is written to the CMS files named in the FNMLG1 and FNMLG2 FILEDEF statements in the NPM startup EXEC. To process NPM VM data in the Analyzer, you must:

- o Ensure that your NPM systems programmer is collecting the data you need to process. See NPM Initialization Statements and Commands below for more information.
- o Transport the CMS files named on the FILEDEF statements to your CA MICS z/OS host using any data transfer product you choose.
- o Modify the DAY056 step of the CA MICS DAILY operational job following the instructions in Section 7.3.2 of this guide.

NPM Initialization Statements and Commands

At activation, NPM reads a set of initialization statements and, if specified, executes a set of initialization commands. The initialization statements define data collection intervals, what data can be collected, and to what destinations the data can be written. The initialization commands enable you to measure specific resources at specific intervals and on a daily basis without the need for operator intervention.

This section covers only those initialization statements and commands for NPM that directly affect the data input to CA

MICS. Refer to the IBM Tivoli NetView Performance Monitor documentation for a complete description of NPM initialization statements and commands.

Sample NPM Initialization Statements

NPM Initialization Statement: HOSTCOLL=YES indicates that this NPM will support data collection from this host.

INTERVAL=(225,SEC): The NPM base INTERVAL is 225 seconds. Seven additional higher intervals, each twice the value of the previous interval, are derived from this base interval for network data collection and exception monitoring commands. The higher intervals that can be derived from a base interval of 225 seconds include the following:

Interval 2	450 seconds (or 7 1/2 minutes)
3	15 minutes
4	30 minutes
5	1 hour
6	2 hour
7	4 hour
8	8 hour

Each command or panel used to start network collection allows you to specify the NPM computed interval, as explained in the example above, designating the frequency of data collection.

Session data collection time intervals use the SESSINT parameter in conjunction with the NPM base INTERVAL value to calculate the length of the session data collection interval. The SESSINT parameter should not be confused with the intervals computed by NPM for network data collection.

Following the example above, where 225 was the NPM base interval in seconds, SESSINT=4 specifies that session data is collected at 15-minute intervals. The SESSINT value of 4 is not the same as interval 4 for network data collection. NPM derives this 15-minute session collection interval by multiplying the value of SESSINT (4) by the base interval (225).

SYNCH=(3,59): NPM interval 3 (15 minutes) ends at 14, 29, and 59 minutes after the hour. The session collection intervals end at the same times. Synchronizing collection intervals to terminate at least one minute before the hour ensures that the data falls into the right hour in CA MICS. For example, data collected for the interval beginning at 8:44 and ending at 8:59 will fall into the hour 8. If the

interval was synchronized to expire at exactly 9:00, then data collected between 8:45 and 9:00 would fall into the hour 9.

NETWORK=(SMF,VSAM): Network data from START COLLECT and START MONITOR commands is written to both SMF and to the NPM REVIEW File. Although multiple destinations are specified in this example for the NPM network data, CA MICS only processes the data written to SMF.

SESSION=(SMF,VSAM): Session interval records generated by SESSCOLL (Session collect) commands are written to both SMF and the Session Statistics File, a VSAM key-sequenced data set. Although multiple destinations are specified in this example for the NPM session data, CA MICS only processes the data written to SMF.

NSA=(SMF): Network session accounting records generated by the NCP for LU sessions are written to SMF. To generate network session accounting records, you must also specify NPA=YES and SESSACC=YES on the BUILD macro in the NCP source definition statements.

```
NPM  HOSTCOLL=YES,
      INTERVAL=(225,SEC),SESSINT=4,SYNCH=(3,59),
      LOG=SMF,NETWORK=(SMF),
      SESSION=(SMF),NSA=(SMF)
```

SESSCOLL Initialization Statement: BVAL=(1,3,5,10):
Default boundary values (BVAL) for the distribution groups for logical unit session transit times have been set to 1, 3, 5, and 10 seconds. For example, if operator (total) response time is 3 seconds, then the counter for distribution group 2 (3 seconds) is incremented.

HOST=900, NET=900, OPER=900: The HOST, NET, and OPER operands specify 900 seconds as the maximum session transit time thresholds for host, network, and total response events. In the example below, host, network, and total response times greater than 900 seconds are discarded to prevent these excessive response times from skewing average response time and other calculated response time values.

```
SESSCOLL  BVAL=(1,3,5,10),
           HOST=900,
           NET=900,
           OPERATOR=900
```

Sample Network Initialization Command

NPM initialization commands execute at NPM activation.
Through the use of the DAILY and CLOCK parameters, you can also define the initialization commands to start and stop each day, even though NPM is kept active on a continuous basis. In the example below, NPM collects data on all lines attached to NCP01 from 6 a.m. until 10 p.m. Collection interval 3 is 15 minutes because the base interval is defined as 225 seconds in the initialization statements above. The network collection records are written to the sequential log, which is defined as SMF in the initialization statements.

```
NETCOLL NCP=NCP01,OPTIONS=START,RESOURCE=ALLNAMES,  
        CLOCK=(06,22),DAILY=YES
```

Sample Session Initialization Command

In the example below, NPM collects session statistics on any logical unit in session with NPM. The session collection interval, 15 minutes, is defined above in the initialization statements. The data for sessions is started dynamically for sessions that are currently inactive.

```
SESSCOLL APPL=NPM,BVAL=(1,3,5,10),DYNAMIC=YES,  
        HOST=900,NET=900,OPERATOR=900
```

The following sections discuss features of NPM:

- 1 - NPM Network Collector Function
- 2 - NPM Session Collector Function
- 3 - NPM Network Session Accounting
- 4 - NPM Network Gateway Accounting

6.1.1.1 NPM Network Collector Function

The NPM Network Collector Function records volume, performance, and reliability data, as collected in the Network Control Program (NCP), which is the communication controller's operating system.

NPM communicates with the Network Performance Analysis Logical Unit (NPALU) in the NCP to retrieve data and record it in one of three places:

- o A review file, which CA MICS does not process
- o The network log
- o SMF records

In z/OS, the data recorded by the NCP is transmitted to the host processor and is written by an NPM host-based routine into the SMF data set.

In VM, the SMF equivalent type 28 records are written to the CMS files named on the FNMLG2 FILEDEF statements in the NPM startup EXEC. It is your responsibility to transport the VM NPM log files to your CA MICS z/OS host.

The NPM Network Collector Function builds a review file and the NPM Network Log. The Network Log can be written to a sequential log file or the SMF data set. For VM NPM, the Network Log can be written to an SMF-equivalent CMS file.

The CA MICS Network Analyzer Option requires that the data be in SMF or SMF-equivalent form (SMF type 28 for NPM). It is your responsibility to archive SMF data on a regular basis for input to CA MICS DAILY update process. If you are running VM NPM, it is also your responsibility to transport the data to your CA MICS z/OS host.

6.1.1.2 NPM Session Collector Function

NPM Session Collector Function gathers response time and loads data at its VTAM interface. Once there, NPM intercepts the VTAM buffer trace module and saves information from the buffer trace in CSA until the session collection interval expires. At this point, the data in CSA is assembled and recorded. The NPM Session Collector Function records response time and loads data to the NPM SMF type 28 record, as well as to the Session Statistics File, which is a key-sequenced VSAM file. NPM session data can be input to CA MICS network only in SMF format.

For VM, NPM Session Collector Function records response time and loads data in SMF type 28, subtype '20'X. It is also your responsibility to transport the VM SMF-equivalent type 28 records to your CA MICS MVS host. No special preparation is required.

Controlling the Volume of Data

The NPM Session Collector Function initiates a VTAM buffer trace for each resource requested by the Session Collection command. As a result, CSA storage and direct access storage space that is needed to contain this data for all logical units (LUs) on a medium-to-large network is prohibitive. Therefore, NPM provides the data center with the ability to record data for selected network components only. You can use both the SESSCOLL command, which is invoked at NPM initialization, and the Start Session Collection screen to limit the data to specific LUs. You can also choose to specify all LUs that are associated with specific nodes (including local NCPs, cross-domain NCPs, local hosts, and cross-domain hosts), applications, or virtual routes.

Network Response Time and Definite Response

NPM's network response time (transit time in NPM terms) is an approximation of the time each transaction spends in the network. It is only measured by the NPM session collection function for transactions that specify definite response (DR).

It is your responsibility to activate DR for any transactions that require network response time.

6.1.1.3 NPM Network Session Accounting

NPM Network Session Accounting collects connect time and traffic statistics for terminal sessions. This information is gathered from the NCP NPALU (Network Performance Analysis Logical Unit). NPM Network Session Accounting differs from NPM Network Collection (also derived from the NPALU) in the following major respects:

- o Network session accounting identifies each session's partners, that is, PLU and SLU.
- o Network session traffic statistics are for LU sessions and never include line overhead, such as polling and retransmissions.

NPM writes network session accounting data to the SMF type 28 record, subtypes '50'X, '51'X, and '52'X, which CA MICS processes. It is your responsibility to archive SMF data on a regular basis for input to CA MICS DAILY update process. If you are running VM NPM, then it is also your responsibility to transport the VM SMF-equivalent type 28 records to your CA MICS MVS host.

6.1.1.4 NPM Network Gateway Accounting

NPM Network Gateway Accounting collects connect time and traffic statistics for cross-network LU-LU sessions. This information is gathered from the gateway NCP NPALU (Network Performance Analysis Logical Unit).

NPM writes Network Gateway Accounting data to the SMF Type 28 record, subtypes '60'X, '61'X, and '62'X, which CA MICS processes. It is your responsibility to archive SMF data on a regular basis for input to CA MICS daily update process. If you are running VM NPM, then it is also your responsibility to transport the VM SMF-equivalent type 28 records to your CA MICS MVS host.

6.1.2 NetView Session Monitor (NLDM)

Tivoli NetView Session Monitor is an operational performance tool used to monitor and manage day-to-day network operations.

The CA MICS Network Analyzer supports NetView Session Monitor. NetView Session Monitor writes type 39 record to the SMF external log.

Some of NetView's functions include collecting, displaying, and recording session response time data by requesting and accepting response time data from the Response Time Monitor (RTM).

NetView records response time data in the NetView external log record (SMF type 39, subtypes 1, 2, 4, and 5). The NetView Session Monitor records session configuration, data traffic, connect, and VTAM Bind failure information in the SMF type 39, subtypes 2, 3, 4, 5, and 6 records. This information is referred to as NetView accounting and availability data.

The CA MICS Network Analyzer supports NLDM data from the following SMF type 39 records and tables:

Record	Hex	Comprised of tables *
RTM Collection	'01'	41 42 43 45 47 48 54 55
Session End	'02'	41 42 43 45 47 48 49 54 55
Session Start	'03'	41 42 43 45 48 49 54 55
Accounting and Availability	'04'	41 42 43 45 49 54 55
Combined Session Start and End	'05'	41 42 43 45 47 48 49 54 55

Table Number	Data Section Supported
42	Product
45	Session Configuration
47	Response Time

	48	Route	
	49	Accounting & Availability	
+-----+			

* if a record is comprised of a table that is not supported by the Analyzer, that table's segment is skipped when the record is read.

The INPUTSMF DD statement specifies the data set name for the NetView Session Monitor/NLDM files. You must provide an archive file that contains the SMF type 39 records for daily processing by CA MICS.

Response Time Monitor (RTM)

Response Time Monitor (RTM) is provided in 3174 and 3274 cluster controllers. This function includes a specific microcode support level and a hardware timer adapter card that is read by the microcode. NetView/RTM data includes average response time, a count of the responses that occurred within user-defined response distribution times, and an indicator of whether installation-defined service objectives were met during the data recording interval.

Since service objectives may be defined differently for different network users, NetView/RTM permits the installation to define performance classes and to associate each response objective with a specific performance class. A performance class can be anything the installation defines, from a group of sessions attached to a particular cluster controller to all TSO sessions. Performance classes are established using the NetView PCLASS and MAPSESS definition statements.

When the NetView/RTM function is activated, the SMF type 39 record will be written at user-defined intervals and at session termination. The NetView COLLECT command is used to produce type 39 subtype 1 records on an interval basis. To implement this feature, the installation must build and invoke an NCCF CLIST to issue the COLLECT command at periodic intervals.

NetView/RTM data is produced only for cluster controllers with the microcode update and for sessions specifically requested through the PCLASS and MAPSESS definition statements. In addition, interval records are produced only periodically by an NCCF CLIST.

NetView Accounting and Availability (A/A)

NetView Accounting and Availability (A/A) measurement data consists of statistical data on user sessions, including connect time, message and data traffic counts, configuration data, and BIND failure information.

When the NetView A/A function is activated, an SMF type 39 record is written at session start, at session end, at user-defined intervals, and when a session is rejected due to a BIND failure. The NetView RECORD command is used to produce type 39 subtype 5 A/A records on an interval basis. To implement this feature, the installation must build and invoke an NCCF CLIST, which issues the RECORD command at periodic intervals.

RTM and A/A Coordination Issues

Note that the NetView COLLECT command, which requests the production of SMF type 39 subtype 1 records containing RTM data, and the NetView RECORD command, which requests the production of SMF type 39 subtype 5 records containing A/A data, are not automatically synchronized. Thus, the data recorded for each function may represent information from different time periods.

If you wish to compare RTM and A/A data for a given user session, you must ensure that the COLLECT and RECORD commands are invoked together. This does not completely ensure that data from each source is for the same time period, but it is the surest way to attempt such correlation of data. (RTM and A/A data are both included in the session termination record, assuming they are both being collected.)

Collecting Data

To activate data collection for the NetView Session Monitor Response Time Data Function, define three of the INITMOD statements in the AAUPRMLP member of the DSIPARM data set as follows:

```
INITMOD AAUINLDM RTM=YES  
INITMOD AAUINLDM SAW=YES  
INITMOD AAUINLDM LOG=YES, SESTATS=???
```

Code SESTATS=NO (above) to the external log if you want NetView Session Monitor/NLDM to write only response time data and not Accounting and Availability data.

Code SESTATS=YES if you also want NetView Session

Monitor/NLDM to log only Accounting and Availability data to the external log.

You must code SAW=YES to collect any data from NetView Session Monitor/NLDM. Coding SAW=YES activates session awareness data collection, which is necessary for collecting any other data.

To activate data collection only for NetView Session Monitor, or the NLDM Accounting and Availability Measurement Data Function, define two of the INITMOD statements in the AAUPRMLP member of the DSIPARM data set as follows:

```
INITMOD AAUINLDM RTM=NO
INITMOD AAUINLDM SAW=YES
INITMOD AAUINLDM LOG=YES, SESTATS=YES
```

You do not need to activate the global trace options (by coding TRACELU=YES or TRACESC=YES in the NetView Session Monitor or NLDM INITMOD statements) or the specific trace (via the NetView Session Monitor/NLDM TRACE command) to collect response time data or accounting and availability data. Activating the global trace may significantly increase the system resource usage.

Collect Response Time Monitor (RTM) data at regular intervals via the NetView Session Monitor/NLDM COLLECT command. If you use the sample CLIST (AUTOCOLL) supplied with NetView Session Monitor/NLDM for RTM data collection, do the following:

- o Change the NOLOG parameter to LOG in the CLIST to log RTM data to SMF.
- o Modify the CLIST so that the COLLECT command does not execute exactly at the hour change. For example, the last COLLECT command in an hour should execute five minutes before the hour change so that the SAS use of the end time stamp does not cause the data from the last collect command in the hour to be placed in the next hour's data.

Collect Accounting and Availability (A/A) data at regular intervals via the NetView Session Monitor/NLDM RECORD command. If you use the sample CLIST (AAUCLACT) that is supplied with NetView Session Monitor/NLDM for A/A data collection, modify AAUCLACT so that the RECORD command executes before each hour change.

6.1.3 NetView Hardware Monitor/NPDA

Tivoli NetView Hardware Monitor/NPDA provides diagnostic and reliability data, including component error statistics and traffic volume. Its online functions are designed to assist network operations in resolving problems quickly.

The CA MICS Network Analyzer Option supports NetView Hardware Monitor, which writes the SMF type 37 reports record containing the following data types:

- o Statistics are records of communications traffic and temporary (recoverable) errors.
- o Events (generic and standard) are either specific errors reported by communications devices or statistics that exceeded the data-center-defined threshold for the error-to-traffic ratio.
- o Alerts are events that qualify for alert status as a result of the analysis by a user-defined Alert recording filter.

The CA MICS Network Analyzer Option supports data from the following SMF type 37 tables:

Table Number	Report Format Supported
27	Product
28	Alert
29	Generic Event
30	Event
31	Statistical
36	LAN

To log NetView Hardware Monitor/NPDA records to SMF, follow the procedures in the OPERATOR=900 Tivoli Netview documentation for writing the type 37 record to the SMF external log. Also, tailor the NetView Hardware Monitor's recording filters to control the quality and the volume of data recorded.

See the Tivoli NetView Online help to define SRATIO, which sets the error-to-traffic ratio thresholds for generating alert messages, and SRFILTER, which controls what data is recorded.

6.1.4 CA NetSpy

CA NetSpy is a VTAM (Virtual Telecommunications Access Method) application that monitors host and network performance. The CA MICS Network Analyzer Option supports the z/OS and VM versions of CA NetSpy.

The CA MICS Network Analyzer Option supports the following CA NetSpy data:

+-----+-----+-----+-----+-----+-----+	
	Offsets
	12 71 72 73
Data Type	-----
Resource Name	Values:
=====	
NCP	
NCP Resource	80 __ 80 02
Line, Controller, Terminal	
Remote BSC Link	40 __ __ 01
Remote BSC Cluster	20 __ __ 01
Remote BSC Terminal	10 __ __ 01
Local Cluster	28 __ __ 01
Local Cluster	88 __ __ 01
Local SNA	89 __ __ 01
Local SNA	29 __ __ 01
Local ?	18 __ __ 01
Local SNA LU	19 __ __ 01
NPA Pseudo Link	43 __ __ 01
NPA Pseudo Dev	03 __ __ 01
Remote SDLC Link	41 __ __ 01
Remote SDLC Physical Unit	21 __ __ 01
Remote SDLC Logical Unit	11 __ __ 01
Switched SDLC Link	85 __ __ 01
Switched SDLC Physical Unit	25 __ __ 01
Switched SDLC Logical Unit	15 __ __ 01
X.25 Link	47 __ __ 01
X.25 Physical Unit	27 __ __ 01
X.25 Logical Unit	17 __ __ 01
CLA - Link	49 __ 40 01
CLA - Physical Unit	29 __ 40 01
NPSI	
X.25 Machine Link	49 04 80 04
X.25 Machine Physical Unit	29 04 40 04
X.25 Virtual Connection	29 04 20 04
+-----+-----+-----+-----+-----+-----+	

continued

continued from prior column

	Offsets
	12 71 72 73
Data Type	-----
Resource Name	Values:
=====	=====
NTRI	
Logical Link	70 08 80 03
Physical Link	71 08 40 03
TIC3 (ODLC)	
Physical Link	49 00 40 07
Physical Unit	29 00 08 07
Frame Relay	
Physical Link	49 02 80 05
Logical Link	49 02 40 05
Physical Unit	29 02 20 05
LMI Station	29 02 10 05
Type A Record (Application)	not applicable
Type B Record (VTAM Buffers)	not applicable
Type C Record (Accounting)	not applicable
Type I Record (TCP Connection)	not applicable
Type J Record (TCP/IP Stack)	not applicable
Type S Record (Terminal Session)	not applicable
Types T and U (Terminal)	not applicable
Type X Records	88
General Alerts:	
Application Program	00
NCP	04
Line	08
Cluster	0C
Logical Unit	10
Virtual Route	14

CA NetSpy is divided into three components: the VTAM interface, the NCP (network control program) interface, and the TCP/IP interface. The VTAM interface collects response time and traffic statistics for host applications and their session partners. The NCP interface collects network traffic, utilization statistics, and network session accounting data from the NCP NPA Logical Unit (NCP NPALU) in front-end processors running NCP or equivalent software. The TCP/IP interface collects information for stacks, and all the UDP, IF, and TCP interfaces.

CA NetSpy writes an SMF record, or the VM equivalent, that has a user-defined SMF record number. (Refer to Section 7.2.1 for information on how to specify the SMF record number to CA NetSpy and to the CA MICS Network Analyzer Option.)

This SMF record contains data from the CA NetSpy VTAM interface, NCP interface, network session accounting (NSA) collection function, network gateway accounting (NGA) collection function, Network Token Ring Interface (NTRI) data collection, NCP Packet Switching Interface (NPSI) data collection, Token Interface Coupler-3 (TIC3), general alert function, and TCP/IP interface.

For CA NetSpy running under z/OS, it is capable of writing its NCP, VTAM, and TCP/IP interface data to SMF.

For CA NetSpy running under VM, the SMF equivalent log record is written to the CMS files named in the LOG1 and LOG2 FILEDEF statements in the startup EXEC. In order to process this data by CA MICS, you must transport these CMS data sets to your CA MICS z/OS host. See Section 7.3.2 for details on the modifications you must make to the DAY056 step of your CA MICS DAILY update job to process VM CA NetSpy network data.

The following sections describe how to tailor CA NetSpy to record data to SMF, synchronize interval collection, and collect network accounting data.

Recording Data to SMF

Your administrator specifies the CA NetSpy SMF record number in the INITPRM member of NETSPY.CNTL. The INITPRM member also controls which record subtypes CA NetSpy produces. These initialization parameters take this form:

SMF=record_number SESSION=sesopt TYPEU=uopt

where:

record_number ranges from 128 to 255

sesopt is YES (record subtype S records)
or NO (do not record subtype S records)

uopt is YES (records subtype U records)
or NO (do not record subtype U records)

For TCP/IP data you must code the following:

SNMPHOST ...IF=(Y|N,Y|N),STACK=(Y|N,Y|N),TCP=(Y|N,Y|N),
UDP=(Y|N,Y|N)

The following parameters indicate what type of MIB data is to be collected and whether or not the collected data is to

be logged. The default is to collect and log all data. The first parameter within the parentheses is the collection indicator. Valid values are Y for YES to collect or N for NO not to collect. The second parameter within the parentheses is the logging indicator. Valid values are Y for YES log data or N for NO logging data. The logging indicator is only valid when the collection indicator is Y.

Valid combinations of these two indicators are (Y,Y), (Y,N), and (N,N).

IF=(Y|N, Y|N) This produces the interface table data.
Default: IF=(Y,Y), to collect and log interface table.

STACK=(Y|N, Y|N)
This produces an overview of the stack, which includes summary information on all three groups.
Default: STACK=(Y,Y), to collect and log stack data.

TCP=(Y|N, Y|N) This produces the TCP connection table data.
Default: TCP=(Y,Y), to collect and log TCP connection table data.

UDP=(Y|N,Y|N) This produces the UDP connection table data.
Default: UDP=(Y,Y), to collect and log UDP connection.

The TCIPMON=YES must be coded before the first SNMHOST initialization parameter.

To process CA NetSpy data in CA MICS, indicate all of the SMF record numbers you have chosen for the various CA NetSpy monitors running on different systems. The default CA NetSpy record for CA MICS processing is 132 (decimal). If you choose an SMF record number other than the default, you must update sharedprefix.MICS.GENLIB(SNTGENIN) with the numbers you choose. Complete directions on how to perform this update is provided in Section 7.2.1.

If you are processing data from VM NetSpy, then you are also responsible for transporting the SMF equivalent data to your CA MICS z/OS host. Use the NetSpy/VM HOSTID parameter to stamp each record with an SMF system identifier, so that once the data is sent to an z/OS host, it can be processed into CA MICS without further modification. The host identifier must

be specified in the CA NetSpy parameters, or it will default to the first four characters of the VTAM host name. If more than one VM system has the same default HOSTID value, those multiple VM systems will have the same SYSID written to the SMF data. This could affect how the CA MICS Network Analyzer Option processes the data, producing unexpected results such as calculated time elements with negative values or events that seem to be duplicates but that actually occurred on different VM systems.

For additional information on the HOSTID parameter, see the CA NetSpy documentation.

SMF Record Subtypes

SMF Record	CA NetSpy	Data Descriptions	
Subtypes	Release(s)		
=====			
S	up through 7.0	Terminal Session	
		Statistics	
T/U	up through 7.0	Terminal Statistics	
A	up through 7.0	Application	
		Statistics	
B	up through 7.0	VTAM Buffer	
		Statistics	
C	up through 7.0	Network Accounting	
		Statistics	
N	up through 7.0	NCP Interface	
		Statistics	
X	up through 7.0	General Alerts	
		Statistics	
V	up through 7.0	Virtual Routes	
		Statistics	
I	up through 7.0	TCP/IP Connection	
		Statistics	
J	up through 7.0	TCP/IP Stack	
		Statistics	

+-----+

A special utility is provided with CA NetSpy that converts CA NetSpy NCP data into CA NetSpy SMF record format, subtype N to SMF type 38 record format, which is the format that NPM network subsystem produces. The purpose of this utility is to provide users who are converting from NPM to CA NetSpy with a convenient way to produce NPM network reports from CA NetSpy data.

Use of the above utility is not required to process CA NetSpy NCP data into CA MICS and it is not recommended because it requires an extra pass of the CA NetSpy NCP data.

Synchronizing Interval Collection

Coordinate with your CA NetSpy administrator to synchronize the collection of CA NetSpy interval data for two important reasons:

- o First, you may want to correlate CA NetSpy data with information from another source, such as the CA TSO/MON PM monitor. By synchronizing collection so that CA NetSpy and CA TSO/MON PM records are written at about the same time, you will be able to compare and combine information from the two monitors for a more complete analysis.
- o Second, because CA MICS records all information based on the end timestamp of records it processes, and because summarization for the DAYS and WEEKS timespans is by HOUR, it is necessary to ensure that the last record of the hour is recorded within the hour in which the activity occurred. If the record is written at or after the hour, the information in the record will be erroneously associated with the subsequent hour.

To synchronize production of CA NetSpy data, use the SYNC statement in the INITPRM member of NETSPY.CNTL. With the SYNC parameter, you tell CA NetSpy the time after the hour at which you want logging synchronized. For example, if you specify a CA NetSpy recording interval (INTERVAL) of 15 minutes and a SYNC parameter of 14:00, then records will be logged at 14, 29, 44, and 59 minutes after the hour.

You may have to experiment with this value to ensure that data is being recorded in the correct hour, because CA NetSpy is not always successful in writing SMF records at precisely the time you request.

Collecting Additional CA NetSpy Data

- o For information on how to activate CA NetSpy NTRI (Network Token Ring Interface), NPSI (NCP Packet Switching Interface), Frame Relay, and TIC3 (Token Ring Interface Coupler) data collection, refer to the CA NetSpy Network Performance Administrator Guide.

The following sections discuss features of CA NetSpy:

- 1 - CA NetSpy VTAM Interface
- 2 - CA NetSpy NCP Interface
- 3 - CA NetSpy TCP/IP Interface
- 4 - CA NetSpy Network Session Accounting
- 5 - CA NetSpy Network Gateway Accounting
- 6 - CA NetSpy General Alerts
- 7 - CA NetSpy-to-CA NetSpy Communication
- 8 - CA NetSpy Data Considerations

6.1.4.1 CA NetSpy VTAM Interface

CA NetSpy VTAM Interface records response time and loads data in an SMF user record, or the VM equivalent. Recording is for site-selected host applications (for example, TSO, IMS, and CICS) and terminal sessions with those applications.

The resulting SMF type data consists of up to five record subtypes, one that contains load and response data by application, three that contain terminal session load and response information, and one that contains virtual route activity and response time data. These records are written at user-defined intervals and their content may be tailored to include information for specific resources.

The CA NetSpy VTAM Interface is similar to the NPM Session Subsystem in function and in information provided. However, there are enough differences in the actual data provided that three CA MICS Network Analyzer Option files are used to accommodate the data. The files containing only CA NetSpy data are:

- o CA NetSpy Application (PLU) File (SNTNSP)
- o CA NetSpy Terminal (SLU) File (SNTNSS)
- o CA NetSpy Virtual Route Activity File (SNTNVR)

Network Response Time and Definite Response

Like Tivoli NPM, CA NetSpy records host and network response times. And, like NPM, network response is calculated only for network responses where definite response (DR) is active.

A key feature of CA NetSpy is its ability to activate DR for some or all network responses. This feature, called FORCEDR, is provided as a CA NetSpy initialization option. The user may specify, for each application, the percentage of transactions where the FORCEDR is to be used, from 10 to 100 percent. Use of FORCEDR permits CA NetSpy to calculate network response time with no application overhead or interference, and with minimal line traffic overhead.

Multiple Session Manager Support

Multiple session managers, such as CA TPX Session Management for z/OS, CA Teleview Session Management for z/OS, NetView Access, and others, permit a user at a single terminal to access multiple host applications (for example, TSO, CICS, and IMS) simultaneously. The multiple session manager accomplishes this by establishing a session with the real

terminal, and one or more "virtual terminal sessions" to various applications on behalf of the user.

For terminal sessions of this type, network monitors provide correct host and network information for the session between the real terminal and the multiple session manager, but they cannot report complete information for the virtual terminal sessions between the multiple session manager and the host applications.

CA NetSpy, however, provides a general interface to multiple session manager applications, which permits accurate recording of network response and terminal name for virtual terminal sessions. This is accomplished by having the session manager notify CA NetSpy when a new session is activated or session switching occurs. If you are running a multiple session manager application at your site or are considering implementing one, you should check with the vendor to verify that it will communicate with CA NetSpy using the multiple session manager interface.

An expanded discussion of the effects of multiple session manager products on network information is provided in Section 2.6. A later section in this chapter discusses the CA NetSpy multiple session manager interface in more depth.

6.1.4.2 CA NetSpy NCP Interface

The CA NetSpy NCP Interface records volume, performance, and reliability data that is collected by a function in the Network Control Program (NCP) called the NPA Logical Unit (NPALU). The NPALU collects data and reports it to the CA NetSpy NCP Interface in the same way it performs this function for Tivoli NPM. CA NetSpy then records this data in subtype N of its SMF record (or the VM equivalent).

Information may be collected for one or more NCPs, lines, physical units (PUs), or logical units (LUs). Start parameters within CA NetSpy permit the installation to control the data collected from various NCPs.

Because data from the CA NetSpy NCP Interface is so similar to that provided by Tivoli NPM Network Subsystem, the CA MICS Network Analyzer writes this data directly into four SNA Network files shared with NPM Network data:

- o NCP Link File (SNTNCL)
- o NCP Activity File (SNTNAF)
- o Network Components Activity File (SNTCAF)
- o Network Incident File (SNTNIN)

Information supplied by the CA NetSpy NCP Interface includes the following data types:

- o NCP Data
 -
 - NCP information includes the CCU cycle speed, used cycle time, buffer and channel queue statistics, and the amount of time in slowdown.
- o Line, Controller, and Terminal Data
 -
 - Information for lines, controllers, and terminals includes message and character traffic counts, outbound queue statistics, and poll, error, and retransmission counts.

6.1.4.3 CA NetSpy TCP/IP Interface

The CA NetSpy TCP/IP Interface records volume, performance, and reliability data that is derived from the Management Information Blocks (MIBs). CA NetSpy uses Simple Network Management Protocol (SNMP) interface to read the MIBs that are associated with the stack, and all the UDP, IF, TCP interfaces.

Information may be collected for one or more TCP/IP servers. TCIPMON=YES/NO controls the monitoring of TCP/IP stacks and SNMHOST controls the logging of the TCP/IP related subtypes.

Information supplied by the CA NetSpy TCP/IP interface includes the following data types:

- o TCP Connection (Subtype I)

Telnet data includes activity for each telnet session monitored during the installation defined interval. The information for telnet session includes bytes sent and received counts, retransmission counts, acknowledgements, roundtrip time, etc.

- o TCP/IP Stack (Subtype J)

TCP/IP stack data includes activity for each TCP/IP server monitored during the installation defined interval. The information for TCP/IP stack includes connection counts (active, passive, and failed), retransmission time, receive and send buffer sizes, etc.

6.1.4.4 CA NetSpy Network Session Accounting

The CA NetSpy network session accounting collects connect time and traffic statistics for terminal sessions. It collects this information from the NCP NPA Logical Unit (NPALU). CA NetSpy network session accounting differs from CA NetSpy NCP interface collection (also derived from the NPALU) in the following major respects:

- o Network session accounting identifies session partners (that is, PLU and SLU).
- o Network session traffic statistics are for LU sessions and never include line overhead, such as polling and retransmissions.

CA NetSpy writes network session accounting data to the CA NetSpy user-defined SMF record with a subtype of "C". This record is further divided into these subtypes: "S" for start, "E" for end, and "I" for interval. CA MICS processes each of these subtypes.

6.1.4.5 CA NetSpy Network Gateway Accounting

CA NetSpy network gateway accounting (NGA) function collects connect time and traffic statistics for cross-network LU-LU sessions. It collects this information from the NCP NPA Logical Unit (NPALU) in gateway NCPs.

CA NetSpy writes network session accounting data to the CA NetSpy user-defined SMF record with a subtype of "C". This record is further divided into these subtypes: "S" for start, "E" for end, and "I" for interval. CA MICS processes each of these subtypes.

Processing NGA data has the following benefits:

- o NGA is the only source of accounting data for sessions just passing through your network. For example, you are company B and a terminal in company A's network traverses your gateway NCP to connect to an application in company C's network. Since neither the terminal nor the application for this session resides in your network, no other accounting data sources currently supported by CA MICS can collect on it.
- o The gateway NCP is often the best accounting data source for cross network sessions, because it is the only source that can identify the network IDs for the terminal and the application, determine whether a session is cross network, and determine whether the PLU and SLU names are real or aliases. Without this information, it may be impossible to identify to whom an accounting invoice should be sent.
- o NGA is a flexible network accounting collection function. It can collect data on cross network sessions with virtually any type of SNA terminal (including locally attached, dial-up, or NCP BISYNC).

NGA data collection has the following limitations:

- o Many configuration fields, such as SLULINK and SLUPU, are often missing in the NGA data. This occurs because either the gateway NCP NPALU did not obtain this information or the monitor (NPM or CA NetSpy) did not write the information to SMF.
- o The CA NetSpy interface to multi-session manager products, such as NetView Access, does not apply to CA NetSpy recorded NGA data. This is because the NGA data is gathered by the gateway NCP, which has no interface to

multi-session managers. Consequently, if you collect NGA data for sessions directed through a multi-session manager, the real PLU will not be identified in either the CA NetSpy or NPM NGA data, but only in the multi-session manager.

- o All NGA and NSA data recorded by NPM or CA NetSpy for LU-LU sessions with TSO will contain synonym names for TSO in the data element PLU. This can be easily corrected by coding the CA MICS exit SNTPLURT. Refer to Section 7.10 for a description of SNTPLURT and how it is used to establish a single value for PLU for VTAM applications (such as TSO) for which multiple application (APPL) statements are defined to VTAM.

For more information about CA NetSpy and the network gateway accounting features, refer to the CA NetSpy and the IBM Tivoli NetView Performance Monitor documentation.

6.1.4.6 CA NetSpy General Alerts

CA NetSpy creates general alerts when measurements from either CA NetSpy VTAM interface data or NCP interface data fall outside user-defined thresholds. These alerts are useful for identifying excessive response times, over or under utilized resources, and congested virtual routes.

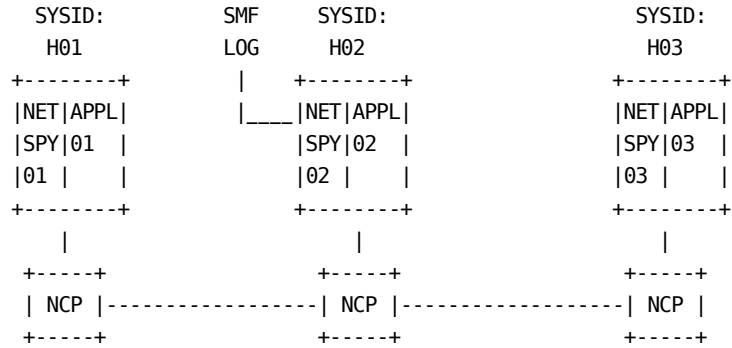
The CA NetSpy user may define these alert thresholds and route them to SMF either through the "Define Monitors" option on the CA NetSpy Main Menu, or by specifying MONITOR statements in the CA NetSpy ALERTPRM member or file. The latter method is recommended for on-going exception monitoring, because MONITOR statements are executed each time CA NetSpy is activated.

CA NetSpy writes general alerts to the CA NetSpy user-defined SMF record with a subtype of X. These records are input into the Network Incident File (SNTNIN) in CA MICS.

For more Information, refer to CA NetSpy Network Performance Administrator Guide.

6.1.4.7 CA NetSpy-to-CA NetSpy Communications

The CA NetSpy-to-CA NetSpy communication interface allows CA NetSpy on one host to communicate with one or more CA NetSpy installations on other hosts.



In the diagram above, CA NetSpys 01 and 03 transmit all network measurement data to CA NetSpy 02, where it is logged to SMF. Because this raw measurement data is sent via the CA NetSpy-to-CA NetSpy interface, no bulk data transfer program is required to provide this central logging of Network SMF data.

In the CA NetSpy SMF data logged on host 02, the SYSID field identifies the host of the CA NetSpy that collected the measurement data on, say, host 01 or 03. For example, CA NetSpy 01 collected response time statistics for APPL01 and then transmitted this data to CA NetSpy 02. When CA NetSpy 02 logs the data to SMF, the SYSID field will identify host 01, the host on which the data was collected. For further information on CA NetSpy-to-CA NetSpy communications, refer to the CA NetSpy documentation.

The CA NetSpy-to-CA NetSpy Communications interface does not create duplicate logging of CA NetSpy data to a single CA MICS system as long as you do not transmit CA NetSpy measurement data to a central site using both CA NetSpy-to-CA NetSpy communications and a bulk data transfer program (or courier system).

6.1.4.8 CA NetSpy Data Considerations

CA NetSpy data will vary depending upon the environment in which CA NetSpy operates and the CA NetSpy processing options your CA NetSpy administrator chose.

The following sections discuss several CA NetSpy options and the effect your CA NetSpy administrator's choices have on the data in the CA MICS database. It also discusses a special CA MICS Network Analyzer option that will eliminate the inflation of character traffic and connect time in certain multiple session manager environments.

Processing Subtype S and U Records

Terminal statistics can be recorded in CA NetSpy record subtypes S, T, and U. Your CA NetSpy administrator controls which records CA NetSpy produces by defining the CA NetSpy initialization parameters in member INITPRM of the partitioned data set CA NetSpy.CNTL. Refer to Section 7.2.1 in this guide.

Target Specification

In the CA NetSpy Application (APPL) statement in the INITPRM member of CA NetSpy.CNTL, you can specify TARGET objective values for response distributions. Specification of TARGET values results in CA NetSpy updating response distributions that indicate how much response time deviates from the average.

You can associate these TARGET values with either HOST response time only or the combination of HOST and NETWORK response time (TOTAL response time), based upon how you specify the TARGETS in the INITPRM member of NETSPY.CNTL:

- o If you specify TARGETS=HOST, the distribution counters are updated with HOST response time only.
- o If you specify TARGETS=USER, the distribution counters are updated only when there is a network response that accompanies a host response.

Response Distributions and CA NetSpy Options

CA NetSpy provides four response distribution targets that you can associate with either host response time only, or total response time (a combination of host and network response). If you specify the CA NetSpy parameter

TARGETS=HOST, then the response distribution fields will be updated whenever a host response is complete, based on the value of the host response time only. If you specify the CA NetSpy parameter TARGETS=USER, then the response distribution fields will be updated based on combined host and network response times.

Once CA NetSpy data is in the CA MICS SNTNSS and SNTNSP files, you can determine which option was selected by examining the common variable RDSTTYPE, which is set to HOST or USER. This will tell your CA MICS administrator whether to associate the response distribution variables (NSSRDST1-5 or NSPRDST1-5) with NSSAVTTM (Average Total Response Time) or NSSAVHTM (Average Host Response Time).

Calculating Total Response Time

It is possible that not all response events have network response time measured for them. This will be true if the CA NetSpy FORCEDR (force definite response) option associated with the APPL parameter is valued at less than 100 (100 indicates that 100 percent of all transactions will have the definite response option activated; 80 indicates that only 80 percent of the responses will have definite response activated, etc.). This will also be true if FORCEDR is not used at all, and not all application transactions use definite response.

CA MICS provides for this in its calculation of total response time and average total response time.

Total network response time is calculated as follows:

- o Average network response time is calculated as the network response time, measured by CA NetSpy, divided by the number of network response events.
- o Then, the average network response time is multiplied by the total number of responses. Total number of responses is set to the greater of network and host responses. So, when there are fewer network responses, the CA MICS Network Analyzer Option simply obtains the average network response and calculates "approximation" of total token response. The measured network response time is kept in fields NSPNRSTM and NSSNRSTM. The calculated value is maintained in fields NSPCNRTM and NSSCNRTM.

Total response time is calculated as the sum of host response time and "calculated" network response time. The average

total response time results from dividing total responses into average total response time.

Multiple Session Manager Considerations

CA NetSpy provides a special interface to resolve the data inflation problems present in a multiple session manager environment. This interface only resolves these problems for the CA NetSpy VTAM Interface data (contained in the terminal activity file and application activity file), and not for the CA NetSpy network session accounting/network gateway accounting data (contained in the NCP network accounting file).

This interface is implemented between the multiple session manager and CA NetSpy whenever a new application session is started, or the user at a terminal switches between applications. The result is that the CA NetSpy terminal record, which represents each virtual terminal session between the multiple session manager and the real application, contains valid network response times and identifies, as the Secondary Logical Unit (SLU), the name of the real terminal that initiated the session through the multiple session manager. CA NetSpy also identifies these records as "virtual terminal" records with a flag. In the CA MICS SNTNSS file, a virtual terminal session is indicated when variable NSSVSESS has a value of Y.

CA NetSpy also sets a "multiple session manager" flag in each application record it produces for a multiple session manager. This flag is carried into the appropriate application and terminal records by CA MICS. The PLUMSMGR flags in the SNTNSS and SNTNSP files are set to "Y" when the application (PLU) is recognized by CA NetSpy as a multiple session manager.

These flags are useful when you want to summarize data in the SNTNSS file by terminal. For example, suppose you want to know the total character traffic, NSSNRBYR plus NSSNRBYS, to terminal T1102015.

The summarization sequence for the SNTNSS file results in an observation for each application (PLU) and terminal (SLU). In the case where a user is logged on to a multiple session manager, has two simultaneous applications (TSO and CICS) active through it, then there are three records in the SNTNSS file for each interval of data. If the real terminal name (SLU) is T110215, then the records are:

Record 1 - SLU=T1102015, PLU= multiple session manager name
Record 2 - SLU=T1102015, PLU= TSO
Record 3 - SLU=T1102015, PLU= CICS

Record 1 contains character traffic information for all data transferred between the real terminal and the multiple session manager (47,255 characters). Records 2 and 3 contain character traffic information for all data transferred between the terminal and each of those applications (21,225 characters for TSO and 24,100 characters for CICS). Note that the session between the real terminal and the multiple session manager recorded 1,900 more characters than the total of the other sessions. This is due to interaction between the terminal user and the multiple session manager.

If you merely summarize the file by terminal name, you will get a total character count of 92,550, approximately double the real traffic to the terminal. Instead, you can use either the NSSVSESS or the PLUMSMGR flag to eliminate the records with the redundant information. If you want to preserve the breakdown by application (TSO and CICS), eliminate records with PLUMSMGR=Y. If you are concerned about accurate network traffic statistics, then eliminate the records with NSSVSESS=Y.

An alternative to remembering to process this data as described above, is to use the SNTOPS parameter "DELETEMS YES" to eliminate the records for the session between the multiple session manager and the real terminal as the raw data is being entered into the SNTNSS file. When this parameter is used, only the virtual terminal records will end up in the SNTNSS file. While this eliminates the possibility of redundant data from improper summarization, it has these drawbacks:

- o Virtual terminal session data is missing the user's interaction with the multiple session manager. It, therefore, can understate the volume of traffic to the terminal.
- o Multiple session manager data compression features actually reduce the amount of data sent to the terminal. Thus, the count of character traffic in the record that is dropped using "DELETEMS YES" may actually be less than that of the combined virtual terminal session records. However, the count in the record dropped more accurately reflects the traffic on the network.

6.1.5 CA NetMaster Network Tracking System (NTS)

CA NetMaster Network Tracking System (NTS) provides services similar to those provided by NetView Session Monitor/NLDM. NTS data is written to the CA MICS NLDM files.

NTS controls the performance class (CA NetMaster RTM class) definitions for the Response Time Monitor (RTM).

NTS is shipped with a sample user exit to write the RTM data to SMF as the type 39 subtype 3 record. Additionally, NTS records session configuration, data traffic, and connect time information in the SMF type 39 subtypes 4 and 5 record. This information is referred to as CA NetMaster accounting data. The CA MICS Network Analyzer Option processes these SMF type 39 record subtypes to add RTM and accounting data to its database.

The INPUTSMF DD statement specifies the data set name for the CA NetMaster input data to the NLDM (Network Logical Data Manager) files. It is your responsibility to provide an archive file that contains the SMF type 39 records for DAILY processing by CA MICS.

Response Time Monitor

The RTM function is provided in the cluster controllers. This function includes a specific microcode support level and a hardware timer-adaptor card that is read by the microcode. CA NetMaster RTM data includes average response time, a count of the responses that occurred within user-defined response distribution times, and an indicator of whether data-center-defined service objectives were met during the data recording interval.

Because service objectives may be defined differently for different network users, NTS permits the data center to define RTM classes and to associate each response objective with a specific RTM class. An RTM class can be anything the data center defines, from a group of sessions attached to a particular cluster controller to all TSO sessions. RTM classes are established using the CA NetMaster RTM class and Session class definitions. NTS RTM classes are equivalent to NetView performance classes and are referred to as performance classes elsewhere in CA MICS documentation.

NTS records all RTM data to the SMF type 39 record, but both NTS and NEWS can initiate collection of the RTM data. NTS collects RTM data at session end and in response to NTS

operator commands to view RTM data on line. Only NEWS allows for collection of RTM data at regular user-defined intervals.

Accounting and Availability

NTS accounting data consists of statistical data about user sessions, including connect time, message and data traffic counts, configuration data, and BIND failure information.

When the NTS accounting function is activated, the SMF type 39 record is written at session start, at session end, and when a session is rejected due to a BIND failure.

NTS does not automatically synchronize periodic collection of RTM and accounting data. Consequently, it can be misleading to compare RTM and accounting data for a given period. For information on how to provide for synchronized collection of RTM and accounting data at regular intervals, see the CA NetMaster documentation.

Your CA NetMaster administrator controls the NTS collection of accounting and RTM data for sessions between network resources through the definition of SAW (Session Awareness), RTM, and Session NTS classes. NTS collects RTM data from terminal controllers only under the following conditions:

- o The terminal controller has the required RTM hardware and microcode installed.
- o Your CA NetMaster administrator defines RTM classes to NTS.
- o Your CA NetMaster administrator defines session classes to NTS that associate the RTM classes to sessions between host applications and terminals with RTM-capable controllers.

Accounting Data Collection

NTS accounting data collection is controlled by the following NTS-dependent CA NetMaster SYSPARM:

NTSACCT = SELECTIVE | ALL | NO

If your CA NetMaster administrator specifies NTSACCT = SELECTIVE, NTS collects accounting data only for sessions that are associated with a SAW class specifying ACCT=YES.

If your CA NetMaster administrator specifies NTSACCT = ALL,

NTS collects accounting data for all network sessions, irrespective of SAW class definitions.

If your CA NetMaster administrator specifies NTSACCT = NO, NTS collects accounting data for no sessions, SAW classes specifying ACT=YES are ignored, and any selective accounting collection ceases.

See the CA NetMaster documentation for SYSPARMS descriptions.

6.1.6 CA NetMaster Network Error Warning System (NEWS)

CA NetMaster NEWS produces NEWS Events and Statistics records that are directed to SMF as the type 37 record through the NEWS NCL &SMFWRITE statement. CA NetMaster NEWS provides data similar to that provided by NetView Hardware Monitor/NPDA.

The CA MICS Network Analyzer requires that this data be in SMF form. It is your responsibility to archive SMF data regularly as input to CA MICS DAILY update process.

CA NetMaster provides two ways of writing SMF type 37 records, and only one of them produces records that can be processed into CA MICS. Coordinate with your site's administrator to be sure that your CA NetMaster produces CA NetMaster SMF 37 records through the use of the CA NetMaster &SMFWRITE exit. The alternative, using the CA NetMaster NEWSXSMF exit, produces SMF records with headers that are incompatible with CA MICS.

Tailor the CA NetMaster NEWS recording options and filters to control the quality and volume of data recorded and define the error-to-traffic ratio thresholds for generating event records.

6.1.7 CA NetMaster for TCP/IP

The CA MICS Network Analyzer processes SMF data generated by the CA NetMaster Network Management for TCP/IP.

All CA NetMaster for TCP/IP information is derived from the Management Information Blocks (MIBs). It uses the SNMP interface to read the MIBs that are associated with the stack, and all the UDP, IF, and TCP interfaces.

Your CA NetMaster for TCP/IP administrator controls the collection of SMF data.

Refer to CA NetMaster for TCP/IP documentation to get information on how to generate its SMF type records.

SMF Record Subtypes

Following CA NetMaster Network Management for TCP/IP subtypes are processed by the CA MICS Network Analyzer:

SMF Record Subtypes	CA NetMaster Network Management for TCP/IP	Data Descriptions
I		TCP Connection Entry
J		Stack Entry

6.1.8 IBM TCP/IP (TCP)

TCP/IP provides statistics for the use of TCP by applications. The applications include Telnet, FTP, and API Calls. TCP/IP allows cross-platform communication in a sysplex.

The CA MICS Network Analyzer supports TCP/IP in an IBM mainframe environment, which writes the SMF type 118 and 119 record types and provides information about the following components:

- o Telnet - records data for Telnet Client and Telnet Server session initiation (logon) and session termination (logoff) statistics.
- o File Transfer Protocol (FTP) - records data for FTP Client and FTP Server commands issued, for example, STOR, RETR, REN, DELE.
- o API Calls - records data for API Calls or TCP initiation as well as termination statistics.

To log IBM's TCP/IP records to SMF, see the IBM documentation for TCP/IP. Since z/OS 1.2, you can log SMF 118 or the new SMF 119, or both. Refer to Section 7.2.1 for information on how to specify the SMF record number for TCP/IP to the CA MICS Network Analyzer.

You may have both TCP/IP SMF records (118 and 119) defined to CA MICS Network Analyzer. To avoid duplicate data in the CA MICS database files, the CA MICS Network Analyzer lets you process only one SMF record type for a unique ORGSYSID. This is accomplished by coding this statement:

IBMTCP SMF = nnn, where nnn is either the 118 or 119

Refer to Section 7.3.1 for information on coding guidelines.

A message will be issued to inform you of the presence of TCP/IP data detected from SMF records that are not defined in the prefix.MICS.PARMS(SNTOPS). This situation can arise when the system programmer makes a switch from SMF 118 to SMF 119 (or vice versa), before you can update the SNTOPS member to reflect the switch that has taken place.

6.2 Processing Network Monitor Data From VM Hosts

Both VM CA NetSpy and VM NPM network monitor data can be processed by the CA MICS Network Analyzer Option. Both of these products are capable of producing records in a VM environment that are equivalent to those produced by their z/OS counterparts. It is your responsibility to transport these records to the z/OS host where CA MICS DAILY update processing will occur.

For VM CA NetSpy, you must transport the data contained in the CMS files identified in the LOG1 and LOG2 FILEDEF statements in your NPM/VM startup EXEC.

For VM NPM, you must transport the data contained in the CMS files identified in the FNMLOG1 and FNMLOG2 FILEDEF statements in your NPM/VM startup EXEC.

In addition, you must make minor changes to the INPUTSMF member of prefix.MICS.PARMS to cause the OS file containing your VM CA NetSpy and/or VM NPM data to be concatenated into the SMF input stream for the DAY056 step of your CA MICS DAILY update job. These changes are described in Section 7.3.2 of this guide. After running a JCLGENU job to regenerate the JCL to your CA MICS DAILY update job, you will be able to process the network monitor data from your VM hosts.

6.2.1 Tivoli NetView Performance Monitor (NPM)

Tivoli NetView Performance Monitor (NPM) is an operational performance tool used to monitor and manage day-to-day network operations. Its data collection subsystem has the following collection functions:

- o Network collection gathers load, performance, NTRI (Network Token Ring Interface), and NPSI (NCP Packet Switching Interface) data in the Network Control Program (NCP).
- o Session collection gathers response time and load data in the host computer.
- o Network session accounting collection gathers accounting (traffic volumes and connect time) data in the Network Control Program (NCP) for network resources belonging to an NCP's boundary function, for example, terminals and distributed hosts defined to the NCP.
- o Network gateway accounting collection gathers accounting (traffic volumes and connect time) data in gateway NCPs for cross-network sessions.

NPM writes network and session data to SMF as a type 28 record. For the VM versions of NPM, the SMF type 28 equivalent log record is written to the CMS files named in the FNMLG1 and FNMLG2 FILEDEF statements in the NPM startup EXEC. For CA MICS to process this data, you must transport these CMS data sets to your CA MICS MVS host.

In addition, you must make minor changes to the INPUTSMF member of prefix.MICS.PARMS to cause the OS file containing your VM NPM data to be concatenated into the SMF input stream for the DAY056 step of your CA MICS DAILY update job. These changes are described in Section 7.3.2 of this guide. After running a JCLGENU job to regenerate the JCL to your CA MICS DAILY update job, you will be able to process the network monitor data from your VM hosts.

The following sections discuss features of NPM:

- 1 - NPM Network Collection Function
- 2 - NPM Session Collection Function
- 3 - NPM Network Session Accounting Collection Function
- 4 - NPM Network Gateway Accounting Collection Function

6.2.1.1 NPM Network Collection Function

The NPM network collection function records volume, performance, and reliability data as collected in the Network Control Program (NCP), which is the communication controller's operating system.

NPM communicates with the Network Performance Analysis Logical Unit (NPALU) in the NCP to retrieve data that can then be recorded in its review file, the network log, and/or SMF (or the VM equivalent). The CA MICS Network Analyzer is designed to process the SMF type 28 record, or the VM equivalent for NPM.

The NPM Network Subsystem produces many subtypes of the SMF type 28 record. Of these subtypes, CA MICS processes only those that are Interval or Monitor Event Records. Specifically, these are subtypes '10'X, '11'X, '12'X, '13'X, '18'X, '19'X, '70'X, '71'X, '74'X, '75'X, '77'X, 'A0'X, 'A1'X, 'D6'X, 'D7'X, and 'DC'X.

INTERVAL RECORD

The SMF type 28 record (subtypes '10'X, '11'X, '12'X, '13'X, '70'X, '71'X, '74'X, '75'X, '77'X 'A0'X, 'A1'X, 'D6'X, 'D7'X, and 'DC'X) contains load, performance, and reliability data collected within the user-defined time interval specified in the INTERVAL operand of the NPM command. At interval expiration, NPM requests data from the communication controller, which it assembles and records to SMF. More frequent collection results in more precise data, but at a higher processing cost for both the network and the CA MICS Network Analyzer.

MONITOR EVENT/EXCEPTION RECORD/RESOLUTION RECORD

NPM is capable of recording exception conditions recognized by the NCP. Exceptions are recorded in the SMF type 28 subtype '18'X and resolutions in SMF 28 subtype '19'X records.

Note that you must provide an archive file that contains SMF type 28 records for DAILY processing by the CA MICS Network Analyzer.

6.2.1.2 NPM Session Collection Function

The NPM session collection function gathers response time and load data at its VTAM interface. There, NPM intercepts the VTAM buffer trace module and saves information from the buffer trace in CSA until the session collection interval expires. At this point, the data in CSA is assembled and recorded. The NPM session collection function can record response time and load data to the NPM SMF type 28 record (or the VM equivalent), as well as to the Session Statistics File, a key-sequenced VSAM file.

The NPM session data can be input to CA MICS only in SMF format or the VM equivalent (type 28 record, subtype '20'X). Modify the DAY056 step of the CA MICS DAILY operational job following the instructions in section 7.3.2 of this guide to process this data.

CONTROLLING THE VOLUME OF DATA

The NPM session collection function initiates a VTAM buffer trace for each resource requested by the Session Collection command. As a result, CSA storage and direct access storage space that is needed to contain this data for all logical units (LUs) on a medium-to-large network is prohibitive. Therefore, NPM provides the data center with the ability to record data for selected network components only. You can use both the SESSCOLL command, which is invoked at NPM initialization, and the Start Session Collection screen to limit the data to specific LUs. You can also choose to specify all LUs that are associated with specific nodes (including local NCPs, cross-domain NCPs, local hosts, and cross-domain hosts), applications, or virtual routes.

More information is provided in Chapter 9, Operational Considerations.

NETWORK RESPONSE TIME AND DEFINITE RESPONSE

NPM's network response time (transit time in NPM terms) is an approximation of the time each transaction spends in the network. It is only measured by the NPM session collection function for transactions that specify definite response (DR).

It is the data center's responsibility to activate DR for any transactions that require network response time.

6.2.1.3 NPM Network Session Accounting Collection Function

The Tivoli NPM network session accounting function collects connect time and traffic statistics for terminal sessions. It collects this information from the NCP NPALU. NPM Network session accounting differs from NPM network collection (also derived from the NPALU) in the following major respects:

- o Network session accounting identifies sessions partners (i.e., PLU and SLU).
- o Network session traffic statistics are for LU sessions and never include line overhead, such as polling and retransmissions.

NPM writes network session accounting data to the SMF Type 28 record, subtypes '50'X, '51'X, and '52'X. CA MICS processes each of these subtypes.

6.2.1.4 NPM Network Gateway Accounting Collection Function

The NPM network gateway accounting function collects connect time and traffic statistics for cross-network LU-LU sessions. It collects this information from gateway NCP NPALUs.

NPM writes network session accounting data to the SMF Type 28 record, subtypes '60'X, '61'X, and '62'X. CA MICS processes each of these subtypes.

6.2.2 CA NetSpy

CA NetSpy is a VTAM application that monitors host and network performance. It is divided into three components: the VTAM interface, the NCP (Network Control Program) interface, and TCP/IP interface. The VTAM interface collects response time and traffic statistics for host applications and their session partners. The NCP interface collects network traffic, utilization statistics, and network session accounting data from the NCP NPA Logical Unit (NCP NPALU) in front-end processors running NCP or equivalent software. The TCP/IP interface collects Telnet, IF, and UDP statistics.

CA NetSpy running under MVS is capable of writing its NCP and VTAM interface data to SMF. For the VM version of CA NetSpy, the SMF equivalent log record is written to the CMS files named in the LOG1 and LOG2 FILEDEF statements in the CA NetSpy startup EXEC. In order to process this data by CA MICS, you must transport these CMS data sets to your CA MICS MVS Host. See Section 7.3.2 for details on the modifications you must make to the DAY056 step of your CA MICS DAILY update job to process this data.

The following sections discuss features of CA NetSpy:

- 1 - CA NetSpy VTAM Interface
- 2 - CA NetSpy NCP Interface
- 3 - CA NetSpy TCP/IP Interface
- 4 - CA NetSpy Network Session Accounting
- 5 - CA NetSpy Network Gateway Accounting
- 6 - CA NetSpy General Alerts
- 7 - CA NetSpy-to-NetSpy Communication

6.2.2.1 CA NetSpy VTAM Interface

The CA NetSpy VTAM Interface records response time and load data in an SMF user record, or the VM equivalent. Recording is for site-selected host applications (for example, TSO, IMS, and CICS) and terminal sessions with those applications. The resulting SMF type data consists of up to five record subtypes, one that contains load and response data by application, three that contain terminal session load and response information, and one that contains virtual route activity and response time data. These records are written at user-defined intervals and their content may be tailored to include information for specific resources.

The CA NetSpy VTAM interface is similar to the NPM Session Subsystem in function and information provided. However, there are enough differences in the actual data provided that three CA MICS Network Analyzer Option files are used to accommodate the data. The files containing only CA NetSpy data are:

- o CA NetSpy Application (PLU) File (SNTNSP)
- o CA NetSpy Terminal (SLU) File (SNTNSS)
- o CA NetSpy Virtual Route Activity File (SNTNVR)

NETWORK RESPONSE TIME AND DEFINITE RESPONSE

Like IBM's NPM, CA NetSpy records host and network response times. And, like NPM, network response is calculated only for network responses for which definite response (DR) is active.

A key feature of CA NetSpy is its ability to activate DR for some or all network responses. This feature, called FORCEDR, is provided as a CA NetSpy initialization option. The user may specify, for each application, the percentage of transactions for which FORCEDR is to be used, from 10 to 100 percent. Use of FORCEDR permits CA NetSpy to calculate network response time with no application overhead or interference, and minimal line traffic overhead.

MULTIPLE SESSION MANAGER SUPPORT

Multiple session managers, such as IBM's NetView Access, CA Teleview Session Management for z/OS, and others, permit a user at a single terminal to access multiple host applications (for example, TSO, CICS, and IMS)

simultaneously. The multiple session manager accomplishes this by establishing a session with the real terminal, and one or more "virtual terminal sessions" to various applications on behalf of the user.

For terminal sessions of this type, network monitors provide correct host and network information for the session between the real terminal and the multiple session manager, but they cannot report complete information for the virtual terminal sessions between the multiple session manager and the host applications.

CA NetSpy, however, provides a general interface to multiple session manager applications, which permits accurate recording of network response and terminal name for virtual terminal sessions. This is accomplished by having the session manager notify CA NetSpy when a new session is activated or session switching occurs. If you are running a multiple session manager application at your site or are considering implementing one, you should check with the vendor of the product to verify that it will communicate with CA NetSpy via the multiple session manager interface.

An expanded discussion of the effects of multiple session manager products on network information is provided in Section 6.8, Multiple Session Manager Considerations. Section 6.3.11, CA NetSpy Data Considerations, discusses the CA NetSpy multiple session manager interface in more depth.

6.2.2.2 CA NetSpy NCP Interface

The CA NetSpy NCP Interface records volume, performance, and reliability data that is collected by a function in the Network Control Program (NCP) called the NPA Logical Unit (NPALU). The NPALU collects data and reports it to the CA NetSpy NCP Interface in the same way it performs this function for IBM's NPM. CA NetSpy then records this data in subtype N of its SMF record (or the VM equivalent).

Information may be collected for one or more NCPs, lines, physical units (PUs), or logical units (LUs). Start parameters within CA NetSpy permit the installation to control the data collected from various NCPs.

Because data from the CA NetSpy NCP Interface is so similar to that provided by IBM's NPM Network Subsystem, the CA MICS Network Analyzer writes this data directly into four SNA Network files shared with NPM Network data:

- o NCP Link File (SNTNCL)
- o NCP Activity File (SNTNAF)
- o Network Components Activity File (SNTCAF)
- o Network Incident File (SNTNIN)

Information supplied by the CA NetSpy NCP Interface consists of NCP, line, controller, terminal, and alert data.

NCP DATA

NCP information includes the CCU cycle speed, used cycle time, buffer and channel queue statistics, and the amount of time in slowdown.

LINE, CONTROLLER, AND TERMINAL DATA

Information for lines, controllers, and terminals includes message and character traffic counts, outbound queue statistics, and poll, error, and retransmission counts.

6.2.2.3 CA NetSpy TCP/IP Interface

The CA NetSpy TCP/IP Interface records volume, performance, and reliability data that is derived from the Management Information Blocks (MIBs). CA NetSpy uses Simple Network Management Protocol (SNMP) interface to read the MIBs that are associated with the stack, and all the UDP, IF, TCP interfaces.

Information may be collected for one or more TCP/IP servers. TCPIPMON=YES/NO controls the monitoring of TCP/IP stacks and SNMHOST controls the logging of the TCP/IP related subtypes.

Information supplied by the CA NetSpy TCP/IP interface includes the following data types:

- o TCP Connection (Subtype I)

Telnet data includes activity for each telnet session monitored during the installation defined interval. The information for telnet session includes bytes sent and received counts, retransmission counts, acknowledgements, round trip time, etc.

- o TCP/IP Stack (Subtype J)

TCP/IP stack data includes activity for each TCP/IP server monitored during the installation defined interval. The information for TCP/IP stack includes connection counts (active, passive, and failed), retransmission time, receive and send buffer sizes, etc.

6.2.2.4 CA NetSpy Network Session Accounting

The CA NetSpy network session accounting function collects connect time and traffic statistics for terminal sessions. It collects this information from the NCP NPA Logical Unit (NPALU). CA NetSpy network session accounting differs from CA NetSpy NCP Interface collection (also derived from the NPALU) in the following major respects:

- o Network session accounting identifies session partners (that is, PLU and SLU).
- o Network session traffic statistics are for LU sessions and never include line overhead, such as polling and retransmissions.

CA NetSpy writes network session accounting data to the CA NetSpy user-defined SMF record with a subtype of "C." This record is further divided into subtypes "S" for start, "E" for end, and "I" for interval. CA MICS processes each of these subtypes.

6.2.2.5 CA NetSpy Network Gateway Accounting

The CA NetSpy network gateway accounting (NGA) function collects connect time and traffic statistics for cross-network LU-LU sessions. It collects this information from the NCP NPA Logical Unit (NPALU) in gateway NCPs.

CA NetSpy writes network session accounting data to the CA NetSpy user-defined SMF record with a subtype of "C". This record is further divided into subtypes "S" for start, "E" for end, and "I" for interval. CA MICS processes each of these subtypes.

Processing NGA data has the following benefits:

- o NGA is the only source of accounting data for sessions just passing through your network. For example, you are company B and a terminal in company A's network traverses your gateway NCP to connect to an application in company C's network. Since neither the terminal nor the application for this session resides in your network, no other accounting data sources currently supported by CA MICS can collect on it.
- o The gateway NCP is often the best accounting data source for cross network sessions, because it is the only source that can identify the network IDs for the terminal and the application, determine whether a session is cross network, and determine whether the PLU and SLU names are real or aliases. Without this information, it may be impossible to identify to whom an accounting invoice should be sent.
- o NGA is a flexible network accounting collection function. It can collect data on cross network sessions with virtually any type of SNA terminal (including locally attached, dial-up, or NCP BISYNC).

NGA data collection has the following limitations:

- o Many configuration fields, such as SLULINK and SLUPU, are often missing in the NGA data. This occurs because either the gateway NCP NPALU did not obtain this information or the monitor (NPM or CA NetSpy) did not write the information to SMF.
- o The CA NetSpy interface to multi-session manager products (for example, NetView Access) does not apply to CA NetSpy recorded NGA data. This is because the NGA data is gathered by the gateway NCP, which has no interface to

multi-session managers. Consequently, if you collect NGA data for sessions directed through a multi-session manager, the real PLU will not be identified in either the CA NetSpy or NPM NGA data, but only in the multi-session manager.

- o All NGA and NSA data recorded by NPM or CA NetSpy for LU-LU sessions with TSO will contain synonym names for TSO in the data element PLU. This can be easily corrected by coding the CA MICS exit SNTPLURT. Refer to section 6.3.8 for a description of SNTPLURT and how it is used to establish a single value for PLU for VTAM applications (such as TSO) for which multiple application (APPL) statements are defined to VTAM.

For more information about CA NetSpy and NPM Network Gateway Accounting features, refer to the CA NetSpy and Tivoli NPM documentation.

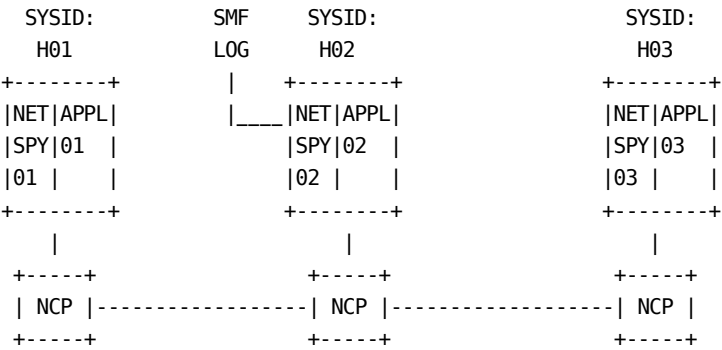
6.2.2.6 CA NetSpy General Alerts

General alerts are created by CA NetSpy when measurements from either CA NetSpy VTAM interface data or NCP interface data fall outside user-defined thresholds. These alerts are useful for identifying excessive response times, over or under utilized resources, and congested virtual routes.

CA NetSpy writes general alerts to the CA NetSpy user-defined SMF record with a subtype of X. These records are input into the Network Incident File (SNTNIN) in the CA MICS Network Analyzer Option.

6.2.2.7 CA NetSpy-to-CA NetSpy Communications

The CA NetSpy-to-CA NetSpy communication interface allows CA NetSpy on one host to communicate with one or more CA NetSpy installations on other hosts.



In the diagram above, CA NetSpys 01 and 03 transmit all network measurement data to CA NetSpy 02, where it is logged to SMF. Because this raw measurement data is sent via the CA NetSpy-to-CA NetSpy interface, no bulk data transfer program is required to provide this central logging of Network SMF data.

In the CA NetSpy SMF data logged on host 02, the SYSID field identifies the host of the CA NetSpy that collected the measurement data, say, host 01 or 03. For example, CA NetSpy 01 collected response time statistics for APPL01 and, then, transmitted this data to CA NetSpy 02. When CA NetSpy 02 logs the data to SMF, the SYSID field will identify host 01, the host on which the data was collected. For further information on CA NetSpy-to-CA NetSpy communications, refer to the CA NetSpy documentation.

The CA NetSpy-to-CA NetSpy Communications interface will not create duplicate logging of CA NetSpy data to a single CA MICS system as long as you do not transmit CA NetSpy measurement data to a central site using both CA NetSpy-to-CA NetSpy communications and a bulk data transfer program (or courier system).

6.2.3 Tivoli NetView

Tivoli NetView is a program product that provides online network management functions and produces information which may be used for management reporting, performance analysis, capacity planning, and network tuning. NetView consists of a command facility, a session monitor, and a hardware monitor. The session monitor and hardware monitor, which are discussed in this section, provide information that is used by the CA MICS Network Analyzer.

NetView is a program product that is built from other program products. The NetView Session Monitor was formerly IBM's Network Logical Data Manager (NLDM). Since the CA MICS Network Analyzer originally supported this product, the information for the NetView Session Monitor file and report names have NLDM as the qualifier. Similarly, since the NetView Hardware Monitor was formerly known as IBM's Network Problem Determination Application (NPDA), the information for the NetView Hardware Monitor file and report names have NPDA as the qualifier. For consistency, all files added in the NetView Session Information Area (NVS) have qualifiers of NLDM.

The following sections discuss the features of the NetView Session and Hardware Monitors:

- 1 - Tivoli NetView Session Monitor/NLDM
- 2 - Tivoli NetView Hardware Monitor/NPDA

6.2.3.1 Tivoli NetView Session Monitor/NLDM

Tivoli NetView Session Monitor, formerly known as the Network Logical Data Manager (NLDM) product, is an operational performance tool used to monitor and manage day-to-day network operations. One of NetView's functions is to collect, display, and record session response time data by requesting and accepting response time data from the Response Time Monitor (RTM), which is a microcode function provided in the 3174 and 3274 cluster controllers. NetView records the response time data in the NetView external log record, which may be written to SMF as the type 39 subtypes 1, 2, 4, and 5 records. The NetView Session Monitor/NLDM also records session configuration, the data traffic, connect, and VTAM BIND failure information in the SMF type 39 subtypes 2, 3, 4, 5, and 6 records. This information is referred to as NetView accounting and availability data. The CA MICS Network Analyzer Option processes the SMF type 39 subtypes 1 through 6 record to add RTM and accounting and availability data to the product database.

The INPUTSMF DD statement specifies the data set name for the NetView Session Monitor/NLDM Files. It is your responsibility to provide an archive file that contains the SMF type 39 records for daily processing by the CA MICS Network Analyzer Option.

RESPONSE TIME MONITOR

The RTM function is provided in the 3274 and 3174 cluster controllers. This function includes a specific microcode support level and a hardware timer adapter card that is read by the microcode. NetView/RTM data includes average response time, a count of the responses that occurred within user-defined response distribution times, and an indicator of whether site-defined service objectives were met during the data recording interval.

Since service objectives may be defined differently for different network users, NetView/RTM permits the data center to define performance classes and to associate each response objective with a specific performance class. A performance class can be anything the data center defines, from a group of sessions attached to a particular cluster controller to all TSO sessions. Performance classes are established using the NetView PCLASS and MAPSESS definition statements.

When the NetView/RTM function is activated, the SMF type 39 record will be written at user-defined intervals and at

session termination. The NetView COLLECT command is used to produce type 39 subtype 1 records on an interval basis. To implement this feature, the data center must build and invoke an NCCF CLIST to issue the COLLECT command at periodic intervals.

NetView/RTM data is produced only for cluster controllers with the microcode update and for sessions specifically requested through the PCLASS and MAPSESS definition statements. In addition, interval records are produced only when the COLLECT command is issued or when it is invoked periodically by an NCCF CLIST.

ACCOUNTING AND AVAILABILITY

NetView accounting and availability (A/A) measurement data consists of statistical data about user sessions, including connect time, message and data traffic counts, configuration data, and BIND failure information.

When the NetView A/A function is activated, the SMF type 39 record is written at session start, at session end, at user-defined intervals, and when a session is rejected due to a BIND failure. The NetView RECORD command is used to produce type 39 subtype 5 A/A records on an interval basis. To implement this feature, the data center must build and invoke an NCCF CLIST, which issues the RECORD command at periodic intervals.

Note that the NetView COLLECT command, which requests the production of SMF type 39 subtype 1 records containing RTM data, and the NetView RECORD command, which requests the production of SMF type 39 subtype 5 records containing A/A data, are not automatically synchronized. Thus, the data recorded for each function may represent information from different time periods. If you want to compare RTM and A/A data for a given user session, you must ensure that the COLLECT and RECORD commands are invoked together. This does not completely ensure that data from each source is for the same time period, but it is the surest way to attempt such correlation of data. (RTM and A/A data are both included in the session termination record, assuming they are both being collected.)

See Section 6.3.9, Important Usage Notes for the NLL and LSY Files, for a more complete discussion of this issue and its effect on data in the CA MICS database.

6.2.3.2 Tivoli NetView Hardware Monitor/NPDA

Tivoli NetView Hardware Monitor, formerly known as the Network Problem Determination Application (NPDA) product, provides you with diagnostic and reliability data, including component error statistics and traffic volumes. Its online functions are designed to assist network operations in resolving problems quickly.

The NetView Hardware Monitor also produces the NetView reports record, which can be directed to SMF as the type 37 subtype 3 record. The CA MICS Network Analyzer processes this SMF record to add diagnostic and reliability data to the CA MICS database.

DATA TYPES

The information recorded by the NetView Hardware Monitor consists of the following:

- o Statistics--records of communications traffic and temporary (recoverable) errors
- o Events (generic and standard)--either specific errors reported by communications devices or statistics that exceeded the installation-defined threshold for the error-to-traffic ratio
- o Alerts--events that qualify for alert status as a result of the analysis by a user-defined Alert recording filter

The installation controls what qualify as events and alerts, and must define these qualifications so that critical information is recorded. The installation also controls the number of NetView Hardware Monitor/NPDA reports records produced through the recording filters.

6.2.4 CA NetMaster

CA NetMaster is an integrated network management software, similar to NetView, that provides online network management functions and produces information that can be used for management reporting, performance analysis, capacity planning, and network tuning. CA NetMaster consists of a group of program products. The Network Tracking System (NTS) and the Network Error Warning System (NEWS) provide information that is used by the CA MICS Network Analyzer Option.

The data provided to CA MICS by the CA NetMaster NTS and NEWS products is equivalent to that provided by the respective NetView Session Monitor/NLDM and NetView Hardware Monitor/NPDA products. Consequently, within the CA MICS Network Analyzer Option, the NTS SMF type 39 data is written to the CA MICS NLDM files and reports, and the NEWS SMF type 37 data is written to the CA MICS NPDA files and reports.

Both NTS and NEWS are required for effective collection of Response Time Monitor (RTM) data. NTS controls performance class (CA NetMaster RTM class) definitions and records RTM data in the SMF type 39 record. NEWS provides periodic collection of RTM data through an EVERY command.

The following sections discuss the features of CA NetMaster NTS and NEWS:

- 1 - CA NetMaster Network Tracking System (NTS)
- 2 - CA NetMaster Network Error Warning System (NEWS)
- 3 - CA NetMaster for TCP/IP

6.2.4.1 CA NetMaster Network Tracking System (NTS)

CA NetMaster NTS provides services similar to those provided by Tivoli NetView Session Monitor/NLDM. NTS data is written to the CA MICS NLDM files. NTS controls the performance class (CA NetMaster RTM class) definitions for the Response Time Monitor (RTM), which is a microcode function provided in the 3174 and 3274 cluster controllers. NTS is shipped with a sample user exit to write the RTM data to SMF as the type 39 subtype 3 record. Additionally, NTS records session configuration, data traffic, and connect time information in the SMF type 39 subtypes 4 and 5 record. This information is referred to as CA NetMaster accounting data. The CA MICS Network Analyzer processes these SMF type 39 record subtypes to add RTM and accounting data to its data base.

The INPUTSMF DD statement specifies the data set name for the CA NetMaster input data to the NLDM Files. It is your responsibility to provide an archive file that contains the SMF type 39 records for daily processing by CA MICS.

RESPONSE TIME MONITOR -----

The RTM function is provided in the 3274 and 3174 cluster controllers. This function includes a specific microcode support level and a hardware timer adapter card that is read by the microcode. CA NetMaster RTM data includes average response time, a count of the responses that occurred within user-defined response distribution times, and an indicator of whether installation-defined service objectives were met during the data recording interval.

Since service objectives may be defined differently for different network users, NTS permits the installation to define RTM classes and to associate each response objective with a specific RTM class. An RTM class can be anything the installation defines, from a group of sessions attached to a particular cluster controller to all TSO sessions. RTM classes are established using the CA NetMaster RTM class and Session class definitions. NTS RTM classes are equivalent to NetView performance classes and are referred to as performance classes elsewhere in CA MICS documentation.

NTS records all RTM data to the SMF type 39 record, but both NTS and NEWS can initiate collection of the RTM data. NTS collects RTM data at session end and in response to NTS operator commands to view RTM data online. Only NEWS allows for collection of RTM data at regular user-defined intervals.

ACCOUNTING AND AVAILABILITY

NTS accounting data consists of statistical data about user sessions, including connect time, message and data traffic counts, configuration data, and BIND failure information.

When the NTS accounting function is activated, the SMF type 39 record is written at session start, at session end, and when a session is rejected due to a BIND failure.

NTS does not automatically synchronize periodic collection of RTM and accounting data. Consequently, it may be misleading to compare RTM and accounting data for a given period. For information on how to provide for synchronized collection of RTM and accounting data at regular intervals, see the NetMaster Network Error Warning System User Reference, Planning and Installation documentation. Also, see Section 6.3.9, Important Usage Notes for the NLL and LSY Files, for a discussion of this issue and its effect on data in the CA MICS database.

6.2.4.2 CA NetMaster Network Error Warning System (NEWS)

CA NetMaster NEWS provides diagnostic and reliability data, including component error statistics and traffic volumes, similar to Tivoli NetView Hardware Monitor/NPDA. NEWS directs this data to SMF as the type 37 subtype 1 record. The CA MICS Network Analyzer Option processes this SMF record to add diagnostic and reliability data to the CA MICS database. NEWS data is written to the CA MICS NPDA Files and processed by the CA MICS standard NPDA reports.

NEWS DATA TYPES

The information recorded by NEWS consists of:

- o Statistics, which are records of communications traffic and temporary (recoverable) errors.
- o Events, which are either specific errors reported by communications devices or statistics that exceeded the site-defined threshold for the error-to-traffic ratio.
- o Alerts, which are events that qualify for alert status as a result of the user-defined Alert recording filters.

The data center controls what qualifies as events and alerts, and typically defines these qualifications so that critical information is recorded. It also controls the number of NEWS SMF type 37 records produced through the recording filters.

6.2.4.3 CA NetMaster for TCP/IP

CA NetMaster for TCP/IP provides information from a non-monitor data source, events. The CA MICS Network Analyzer processes SMF data generated by the CA NetMaster for TCP/IP.

IBM TCP/IP runs as a started task in its own address space. Each of the servers, except Telnet, runs in its own address space and must be started with its own procedure. The Telnet server runs in the same address space as TCP/IP, and is started automatically when TCP/IP is started. You must configure TCP/IP and FTP profiles to collect SMF data for processing in CA MICS Network Analyzer supports.

The information recorded by TCP/IP consists of:

- o CA NetMaster for TCP/IP Identifier
- o Version Number
- o Release Number
- o Maintenance Level

6.2.5 CA MICS Requirements for Data Input

The CA MICS Network Analyzer Option DAILY job requires a single input DD statement: INPUTSMF. NPM network and session data, NetView Session Monitor/NLDM, NetView Hardware Monitor/NPDA, NetMaster NTS, CA NetMaster NEWS, CA NetSpy network and session data, and TCP/IP data are read from the INPUTSMF DD statement. In addition, if you are processing CA NetSpy or NPM monitor data from a VM host, then the names of the OS data sets containing this data must be concatenated to the INPUTSMF DD statement.

Section 7.3.2 describes the specifications for INPUTSMF. Section 7.3.3 describes the update required for the prefix.MICS.PARMS(JCLDEF) SMFRECORDING parameter.

6.3 Correlating Data Sources

The following sections provide information on correlating data sources to reports and CA MICS files.

Each issue is discussed in a separate section. The topics are:

- 1 - Correlating Data Sources to Reports
- 2 - Relationship of Data Sources to CA MICS Files
- 3 - Establishing a Network Identifier (NETWRKID)
- 4 - Defining Time Zone Offsets
- 5 - Establishing TP Circuit Identifier (LNKTPCID)
- 6 - Ensuring All Required Input Data Is Present
- 7 - CA NetSpy and IBM TCP/IP SMF Data
- 8 - Establishing a Single Value for PLU (SNTPLURT)
- 9 - Important Usage Notes for the NLL and LSY Files
- 10- Determining Number of Route Element/TG Names
- 11- CA NetSpy Data Considerations

6.3.1 Correlating Data Sources to Reports

Each CA MICS Network Analyzer Option report, in tabular or exception form, is built using data from a unique input data source. The product does not attempt to mix data from more than one source in any report.

Figures 6-1 and 6-2, Data Sources and Corresponding SNA Network Reports, show which data sources are necessary for which reports.

Data Source/ Record Description	Record Type	Tabular Report	Exception Report
NPM:			
NPM Network Interval	SMF 28	SNT208	12001-12005
		SNT209	12061-12062
		SNT215	
		SNT216	
		SNT401	12121-12124
NPM Network Monitor Event	SMF 28		12181-12209
NPM Session Data	SMF 28	SNT101	12661-12663
		SNT103	12780-12782
		SNT201	
		SNT203	
		SNT403	
NetView Hardware Monitor or CA NetMaster NEWS	SMF 37	SNT601	12541-12542
		SNT602	12601

Data Source/ Record Description	Record Type	Tabular Report	Exception Report

NetView Session Monitor or CA NetMaster NTS with 3274/3174 RTM	SMF 39	SNT105	12301
		SNT111	
		SNT112	
		SNT113	
		SNT114	
		SNT115	12801-12802
NetView Accounting & Availability data or CA NetMaster NTS accounting data	SMF 39	SNT211	12852-12859
		SNT212	12862
		SNT213	
		SNT214	
CA NetSpy NCP Interface	SMF n	SNT208	12001-12005
	where	SNT209	12061-12062
	n is	SNT215	
	user-	SNT216	
	defined	SNT401	12121-12124
CA NetSpy VTAM Interface	SMF A, S, T, and U	SNT121	
		SNT122	
		SNT221	
		SNT222	
CA NetSpy General Alerts	SMF X		12181-12195

Creating Performance Classes for Reporting

Control units (3274s and 3174s) with the Response Time Monitor feature installed measure end-user response time for terminal sessions. This unique feature also allows you to specify response time objectives as the percentage of all transactions being less than a predetermined value (in seconds). For example, a data center determines that the terminals attached to control unit XYZ would provide adequate

service if 90% of all transactions have end-user response times within three seconds. These objectives are defined to NetView Session Monitor or CA NetMaster NTS and to the control unit. If, during a predefined interval (such as 30 minutes), that objective is not met, the control unit and NetView or CA NetMaster record the objective as missed.

Response objectives relate to NetView performance classes and CA NetMaster RTM classes, both of which are referred to here as performance classes. A performance class constitutes any grouping the data center chooses. For example, all users on the same link may belong to a performance class; or, all TSO users may belong to a performance class. With NetView, the data center defines the performance class service objectives, then maps the terminal sessions to the appropriate performance classes using the NetView MAPSESS definition statement. With CA NetMaster, the Session Class definition provides a similar function to the NetView MAPSESS definition statement.

The following reports are based on site-defined performance class:

- o Exception Report 12301, Response Objective Missed for Performance Class
- o Tabular Reports
 - SNT105, NLDM Service by Performance Class
 - SNT115, NLDM Service by Performance Class
- o Sample Graphic - Application Response by Performance Class
- o MICF Inquiries
 - SNTCD1, SNTPD1 - NetView Daily Avg Responses by PCLASS
 - SNTCD4, SNTPD4 - NetView Daily % Resp Within Obj by PCLS

For more information on how to establish and control NetView performance classes, see the descriptions of the PCLASS and MAPSESS definition statements in the NetView documentation. For similar information on CA NetMaster, see the descriptions of RTM classes and Session classes in the CA NetMaster documentation.

6.3.2 Relationship of Data Sources to CA MICS Files

Figures 6-3 through 6-8, Network Data Sources and Associated Files, show the CA MICS files produced from each record type in each data source. This provides a quick way to see which information is missing if you do not produce or process the data from a particular product.

Record Description	Record Type	Network File(s)
Netview Performance Monitor:	SMF 28 subtypes	
NPM Network Interval	hex 11	SNTNCL
	hex 12 & 13	SNTCAF
	hex 10	SNTNAF SNTNLP
NPM Network NTRI	hex 70 & 71	SNTNCL
NPM Network NPSI	hex 74	SNTNCL
	hex 75 & 77	SNTCAF
NPM Network TIC3	hex A0	SNTNCL
	hex A1	SNTCAF
NPM Frame Relay	hex 82, 83, 84, 85	SNTNCL
	hex 82, 83, 84, 85	SNTCAF
NPM VTAM Global	hex D6	SNTVGB
NPM VTAM Buffer	hex D7	SNTVBS
NPM VTAM CSM	hex DC	SNTVCS

Figure 6-3. Network Data Sources and Associated Files

Record Description	Record Type	Network File(s)
Netview Performance Monitor:	SMF 28 subtypes	
NPM Network Monitor Event	hex 18 & 19	SNTNIN
NPM Session Data	hex 20	SNTPSU SNTPSY SNTNPL
NPM Network Session Accounting	hex 50, 51 & 52	SNTNAC
NPM Network Gateway Accounting	hex 60, 61 & 62	

Figure 6-4. Network Data Sources and Associated Files

Record Description	Record Type	Network File(s)
NetView Hardware Monitor/NPDA	SMF 37 subtype 3	SNTNEF SNTNSF SNTGAF SNTLNF
NetView Session Monitor/NLDM	SMF 39 subtypes 1,2,4,5 1,2,4,5	SNTNSV NVSLSY

	2,3,4,5	NVSNSA	
		+-----+	
	2,3,4,5	NVNSC	
		+-----+	
	1,2,4,5	NVSNLL	
		+-----+	
	1,2,3,4,5	NVSRTE	
		+-----+	
	1,2,4	NVSRTM	
		+-----+	
	3,5,6	NVSVBF	
	+-----+	+-----+	

Figure 6-5. Network Data Sources and Associated Files

Record Description	Record Type	Network File(s)
CA NetMaster NEWS	SMF 37 subtype	SNTNEF
	+ 1	SNTNSF
CA NetMaster NTS	SMF 39 subtypes	
	+-----+	
	5	SNTNSV
	+-----+	
	5	NVSLSY
	+-----+	
	5	NVSNSA
	+-----+	
	3,5	NVNSC
CA NetMaster TCP/IP	+-----+	
	5	NVSNLL
	+-----+	
	5	NVSRTE
	+-----+	
	5	NVSRTM
	+-----+	
	5	NVSVBF
CA NetMaster TCP/IP	SMF n subtypes	
	+-----+	
	I	SNTNTS

	J	SNTTCS

Figure 6-6. Network Data Sources and Associated Files

Record Description	Record Type	Network File(s)
CA NetSpy Monitor:	SMF n subtypes	
VTAM Interface data	A	SNTNSP
	B	SNTVBS
	T,U,S	SNTNSS
	V	SNTNVR
Frame Relay data - FRLY	N	SNTNCL
	N	SNTCAF
NCP Interface data	N	SNTNCL
	N	SNTCAF
	N	SNTNAF
NCP Interface data - NTRI	N	SNTNCL
NCP Interface data - NPSI	N	SNTNCL
	N	SNTCAF
NCP Interface data - TIC3	N	SNTNCL
	N	SNTCAF
Telnet Server Entry	I	SNTNTS
Stack Entry	J	SNTTCS
Network Session Accounting & Network Gateway Accounting	C	SNTNAC

CA NetSpy General Alerts	X	SNTNIN

Figure 6-7. Network Data Sources and Associated Files

Record Description	Record Type	Network File(s)
MVS TCP/IP	SMF 118	
Telnet		TCPSTN
		TCPCTN
FTP Server		TCPFSE
FTP Client		TCPFCE
Sockets		TCPAPI
MVS TCP/IP	SMF 119	
	Subtype	
	21	TCPSTN
Telnet Client	23	TCPCTN
FTP Server	70	TCPFSE
FTP Client	3	TCPFCE
FTP Login Failure	72	TCPFLF
TCP Termination	2	TCPAPI
TCP TCP/IP Statistics	5	TCPICX TCPIPX TCPTCI TCPUDI

Figure 6-8. Network Data Sources and Associated Files

6.3.2.1 Example 1 - All Sources (except CA NetSpy)

BASIC ASSUMPTIONS

The estimates in Figures 6-9 and 6-10 are based on data processed from all of the sources that the Analyzer accepts, except for CA NetSpy. The sources for the estimates are:

NPM 1.4 Network - SMF Type 28 Record
NPM 1.4 Session - SMF Type 28 Record
NetView (NLDM) - SMF Type 39 Record
NetView (NPDA) - SMF Type 37 Record

Your estimates will be lower if you are not processing data from all sources.

- o When the CA MICS Network Analyzer is installed, you determine the sort sequence of the SNTPSU, NVSNSA, NVSNSC, NVSRTE, and NVSTRM Files by setting account fields as part of the sort key. You usually choose terminal name or cluster controller name (e.g., 3174) as the lowest level sort key. Depending upon this choice, each observation in each summarized level of the file represents the activity and response for a terminal or a controller.

The choice of this sequence is very important to the overall space required by CA MICS SNA. In Figure 6-11, we assume that the sort sequence of this file is by terminal name. Total space requirements may be as much as 25 percent less than the figures shown if files with accounting fields are kept at the cluster controller level, depending on your exact configuration.

- o Average ACCTs represents the average number of active terminals since we assume that the user-defined sort sequence for these files results in an observation for each terminal. The average is computed as 25 percent of the total number of terminals (represented by the Terminals field on the chart) since it is based on a 24 hour period.
- o This space estimate represents 1 NETWRKID with 1 SYSID and the following number of SAS files per time-span:

FILE	DETAIL	DAYS	WEEKS	MONTHS	YEARS

SNTNCL	03	07	03	03	00

SNTCAF	00	10	03	03	00
SNTNAF	01	10	09	06	00
SNTNIN	33	00	00	02	00
SNTNEF	07	07	09	06	02
SNTNSF	07	07	09	06	02
SNTLNF	07	07	09	06	02
SNTGAF	07	07	09	06	02
SNTPSU	01	03	03	00	00
SNTPSY	00	07	09	06	00
SNTNPL	00	07	09	06	00
SNTNSV	07	07	09	06	02
NVSLSY	00	07	09	06	00
NVSNLL	00	07	09	06	00
NVSRTE	01	05	05	06	00
NVSRTM	01	05	05	06	00
NVNSA	01	05	05	06	00
NVNSC	01	05	00	00	00
NVSVBF	07	07	09	06	00

MODEL PARAMETER VALUES	MODERATE	MEDIUM	LARGE
NCPs (e.g., 37xxs)	1	4	10
Links (lines)	50	100	200
Controllers (e.g., 3274)	100	250	450
Applications (e.g., TS0)	3	6	6
Average # of Application Sessions per Day	1,000	4,000	20,000
Terminals (e.g., 3278)	500	2,000	10,000
Average # of VTAM Abnormal UNBINDS per Day	1,000	4,000	8,000

Average ACCTs in DETAIL	125	500	2,000
Average ACCTs in DAYS	125	500	2,000
Average ACCTs in WEEKS	125	500	2,000
Average ACCTs in MONTHS	125	500	2,000
Average ACCTs in YEARS	125	500	2,000

Figure 6-9. SNA Network Space Estimate Assumptions

MODEL PARAMETER VALUES	MODERATE	MEDIUM	LARGE
NLDM Perform Classes	5	10	15
NPM Network Interval	10 min.	10 min.	10 min.
NPM Session Interval	10 min.	10 min.	10 min.
NLDM RTM COLLECT Interval	15 min.	15 min.	15 min.
NLDM Acct & Availability RECORD Interval	15 min.	15 min.	15 min.
NPDA Temp Errors per Hour	10	15	30
NPDA Failures per Day	10	50	75

Average NPDA			
Error Types	5	10	15

Figure 6-10. SNA Network Space Estimate Assumptions

SPACE ESTIMATES

The space estimates in Figure 6-11 are listed in terms of number of tracks and are based on the parameters indicated in Figures 6-9 and 6-10. The maximum number of tracks on a 3380 is 13,275.

INFO AREA	MODERATE	MEDIUM	LARGE
TIME-SPAN			
DETAIL			
NVS	97	381	1,607
SNT	163	328	697
DAYS			
NVS	437	872	2,614
SNT	623	1,311	3,290
WEEKS			
NVS	254	468	1,330
SNT	609	1,187	2,882
MONTHS			
NVS	49	168	532
SNT	78	159	545
YEARS			
NVS	5	5	5
SNT	0	0	0
NVS	842	1,894	6,088
SNT	1,473	2,985	7,414
TOTAL	2,315	4,879	13,502

Figure 6-11. SNA Network DASD Space Estimates

6.3.2.2 Example 2 - CA NetSpy Only

BASIC ASSUMPTIONS

- o The estimates in Figure 6-12 are based on data processed from CA NetSpy only. The CA NetSpy SMF Record (record number is user defined) contains data from both the CA NetSpy VTAM interface and the CA NetSpy NCP interface.
- o This space estimate represents 1 NETWKID with 1 SYSID and the following number of SAS files per time-span:

FILE	DETAIL	DAYS	WEEKS	MONTHS	YEARS
SNTNCL	03	07	03	03	00
SNTCAF	00	10	03	03	00
SNTNAF	01	10	09	06	00
SNTNSP	03	07	13	13	00
SNTNSS	01	05	05	06	00
SNTNVR	01	05	05	06	00

MODEL PARAMETER VALUES	MODERATE	MEDIUM	LARGE
NCPs (e.g., 37xxs)	1	4	10
Links (lines)	50	100	200
Controllers (e.g., 3274)	100	250	450
Applications (e.g., TS0)	3	6	6
Terminals (e.g., 3278)	500	2,000	10,000
Average # MSM Terminals per day	0	50	100
Average # MSM Applications per day	0	3	4

VRs Monitored	8	16	32
CA NetSpy SMF Interval	10 min.	10 min.	10 min.

Figure 6-12. CA NetSpy Space Estimate Assumptions

CA NetSpy SPACE ESTIMATES

The space estimates in Figure 6-13 are listed in terms of number of tracks and are based on the parameters indicated in Figure 6-12. The maximum number of tracks on a 3380 is 13,275.

INFO AREA	MODERATE	MEDIUM	LARGE
DETAIL			
SNT	220	405	1,016
DAYS			
SNT	354	966	2,973
WEEKS			
SNT	283	681	2,285
MONTHS			
SNT	63	136	463
YEARS			
SNT	0	0	0
TOTAL	920	2,188	6,737

Figure 6-13. CA NetSpy DASD Space Estimates

6.3.3 Establishing a Network Identifier (NETWRKID)

Network Identifier is an eight-character variable, NETWRKID, which is the highest (most significant) sequence/summary variable in each of the CA MICS network files.

Currently, only two of the network monitors supported by the CA MICS Network Analyzer Option, NPM and CA NetSpy (network session accounting/network gateway accounting data only), carry the network name in their records. Because the other monitors do not provide a network name, you must code a unique one-to-eight-character network identifier for each network processed by CA MICS.

For the CA MICS files derived from NPM and CA NetSpy network session accounting, you can set NETWRKID to the value of the NPM/CA NetSpy data field containing the network identifier of the primary logical unit in a session.

The network identifier is used in several places in CA MICS:

- o The highest qualifier in each CA MICS Network Analyzer Option file
- o The CA MICS Tabular Reports and Graphic Inquiry Reports
- o SNTOPS, the CA MICS Network Analyzer options, described in the next chapter

Section 7.3.4, Network Identifier Exit Routine, describes the user routine you must code to establish this variable.

6.3.4 Defining Time Zone Offsets

The purpose of the TIME OFFSET specification is to let you bring data from multiple time zones together in the same CA MICS database unit. In such a case, one of the time zones is selected as the base, and is assigned a TIME OFFSET of 0. The TIME OFFSET for each system in a different time zone from the base is set according to whether the time zone is east or west of the base system:

- o For a time zone west of the base, use a positive number.
- o For a time zone east of the base, use a negative number.

TIME OFFSET is always added to the data time.

Example: A user's hub system is located in New York. A satellite system is located in Chicago. The time zone difference is one hour. The following TIME OFFSET specifications are used:

- o New York - Time Offset 0
- o Chicago - Time Offset 1

Record times, including the time the record was written, interval end-time, and other time-of-day values, are all adjusted using the time offset value specification. The variable TMOFFSET is carried as a retained data element in each file. This can be used to calculate the original time stamps if necessary.

Some of the network monitors (for example, NPM) provide a similar time zone offset capability that takes affect before the data is written to SMF. In such cases, you can adjust the data for different time zones in CA MICS or in the network monitor, but do not make the adjustment in both places. The CA MICS time zone offset adjustment affects all CA MICS Network Analyzer files, not just those files from a specific data source. Consequently, if you process data from multiple network monitors into CA MICS Network Analyzer, and not all of these monitors provide a time zone offset feature, it is better to make the offset in CA MICS.

Section 7.3.1, Product-Specific Parameters (SNTOPS), discusses how to set TIME OFFSET in prefix.MICS.PARMS(SNTOPS).

6.3.5 Establishing TP Circuit Identifier (LNKTPCID)

TP Circuit Identifier is a 14-character variable that can easily be added to the three CA MICS Network Analyzer Link files to document the link vendor's (AT&T, MCI, and so on) billing identifier. This information permits personnel responsible for hardware maintenance to quickly identify the TP Circuit ID associated with a failing link, thus reducing problem reporting and hardware outage time.

This variable, when activated and initialized by the exit routine described in Section 7.3.5, Link TP Circuit ID Exit Routine Definition (SNTCIDRT), can be added to one or more of the following files:

- o NCP Link File (SNTNCL)
- o NPM Link Activity File (SNTNPL)
- o NLDM Link Activity File (NVSNLL)

TP Circuit Identifier is not required. You can omit its definition altogether.

6.3.6 Ensuring All Required Input Data Is Present

The CA MICS Network Analyzer Option is different from most CA MICS components because it processes input data from more than one source. All input data is processed by the DAY056 step in the CA MICS DAILY job as part of the same process. By reviewing the MICSLOG output of the DAY056 step of the CA MICS DAILY job, you can determine exactly what SMF record types and subtypes were present in the input data stream for each of your z/OS or VM hosts.

Following CA MICS standards, if the data center fails to provide input from ANY source, the DAY056 step will fail with a U300 abend. When you expect this problem but must run the DAILY job anyway, SYSPARM=NODATA may be coded on the EXEC statement of the DAY056 step to prevent the abend.

However, there is no parameterized provision in CA MICS to cause a similar abend when data from one of the required sources is missing, but data from other sources is present.

An example will help to illustrate the point. It is Corporation ABC's requirement that NPM Network (SMF Type 28 Record), NPM Session (SMF type 28 record), and NetView Hardware Monitor/NPDA (SMF type 37 record) data be input to the CA MICS Network Analyzer Option on a daily basis. If one of these sources, such as the NPM Session data, is not provided, the DAY056 step should fail so that the data may be located and the update may be run with it.

To provide for this case, the user may code an exit routine, _USRIHL, in which the Input History Log DETAIL File may be examined at the end of DAILY processing. This routine, and a sample exit that provides this function, are documented in Chapter 10.

6.3.7 CA NetSpy and IBM TCP/IP SMF Data

CA NetSpy provides users the flexibility to log SMF data to the record type of their choice. The record type can be any number between 128 to 255. Moreover, a different record type could be selected for CA NetSpy running in different Logical Partitions (LPARs).

IBM TCP/IP can be configured to generate SMF type 118 and 119 records. Your data center may be collecting both of these record types from a single LPAR. At the same time one LPAR can be generating SMF type 118 records while another can be generating SMF type 119 records.

The administrator must determine all record types that are logged to SMF by CA NetSpy and IBM TCP/IP. The administrator then must configure CA MICS Network Analyzer to accept and process them in DAY056 step of the DAILY job.

Refer to chapter 7 for details on how to configure all the SMF record types in `sharedprefix.MICS.GENLIB(SNTGENIN)` and `prefix.MICS.PARMS(SNTOPS)`

6.3.8 Establishing a Single Value for PLU (SNTPLURT)

Some VTAM applications, such as TSO and TAF (Terminal Access Facility, which run under NetView or NCCF), have multiple application (APPL) statements defined to VTAM. Multiple names for a single application in NetView Session Monitor, CA NetMaster NTS, and NPM session data can result, causing two special problems for data in the CA MICS Network Analyzer files:

- o The first problem applies to NetView, CA NetMaster, NPM session, and NPM/CA NetSpy network session accounting/network gateway accounting data for any application with multiple APPL statements defined.
- o The second problem is unique to NetView accounting and availability data and to CA NetMaster accounting data for TSO sessions.

These problems are discussed below.

- o If an application has multiple APPL statements defined, the CA MICS element Primary Logical Unit (PLU) contains different values for different sessions with this application. This can greatly increase the size of files that have PLU as a sequence/summary element. NPM and its session data collection function, if properly tailored, circumvents this problem (discussed below); NetView and CA NetMaster do not address the problem. The affected files are SNTPSY, SNTPSU, SNTNPL, SNTNAC, NVLSY, NVSVBF, NVNSA, NVNSC, NVSRTE, and NVSRM.
- o Two sessions are recorded by NetView and CA NetMaster during every TSO user session: one for the initial session with TCAS and one for the session with a TSO address space. This number is carried in the CA MICS element Number of Sessions (NSCNMSES). Although NSCNMSES is technically accurate, you can think of it, for accounting purposes, as only one session.

You can code the CA MICS Network Analyzer routine SNTPLURT in prefix.MICS.PARMS to convert the multiple PLU values to a single PLU name for the application in NetView, CA NetMaster, CA NetSpy/NPM network session accounting data, and, if required, in NPM session data. SNTPLURT also increments NSCNMSES by one only for each TSO user session. See Chapter 7 for information on how to code SNTPLURT and for examples of how the APPL statements for TSO and TAF are likely to appear in the major node that contains their definitions in

SYS1.VTAMLST.

As indicated earlier, NPM session data collection eliminates the problem of incurring multiple values for the PLU element for applications that have multiple application statements defined. See the parameters SYNCOUNT and SYNMASK in the APPL initialization statement in the NPM documentation.

The SNTPLURT routine is not necessary for data collected by the CA NetSpy NCP interface (except for network session accounting/network gateway accounting data). Moreover, the routine should not be necessary for data collected by the CA NetSpy VTAM interface, as long as you have correctly specified the ALIAS parameter in the CA NetSpy initialization parameters. See the CA NetSpy documentation for additional information.

6.3.9 Important Usage Notes for the NLL and LSY Files

The NLDM System Activity (NVSLSY) File and the NLDM Link Activity (NVSNLL) File combine data from two separate collection functions within the same monitor: either two collection functions within NetView or two collection functions within CA NetMaster. You must ensure that these two data collection functions are synchronized, or the data from the two functions in each file will represent information from different time periods.

To synchronize NetView Response Time Monitor (RTM) data and NetView accounting and availability (A&A) data collection, execute the NetView COLLECT and NetView RECORD commands simultaneously at regular intervals throughout the day using NetView/NCCF CLISTS. The NetView COLLECT command produces the SMF type 39 interval record that contains RTM data and the NetView RECORD command produces the SMF type 39 interval record that contains A&A data.

On NetView hosts that control large network domains, you may not be able to synchronize the collection of RTM and A&A data on a domain-wide basis. For example, if a NetView domain contains 2,000 or more remote 3274/3174 cluster controllers with the RTM feature, several minutes can elapse from the time the NetView COLLECT command executes until the time NetView receives RTM data from all of the remote controllers. A similar delay does not occur when A&A data is received because it is extracted internally from VTAM. A possible solution is to synchronize the collection of A&A and RTM data for a subset of network resources within a NetView domain. For example, if you want to use the data as it is organized in the NLDM Link Activity (NVSNLL) File, synchronize execution of the NetView COLLECT and RECORD commands for all the resources attached to a given NCP or link. If the arrangement of data in the NLDM System Activity (NVSLSY) File is more useful to your data center, synchronize collection of the A&A and RTM data by primary logical unit (PLU).

If both the RTM and A&A data collection functions are turned on in NetView, then RTM and A&A data is automatically forwarded to NetView and combined in a session termination record, even if the data is not actively solicited through COLLECT and RECORD commands. However, it is important to consider producing records for both RTM and A&A data at regular intervals using NetView CLISTS containing COLLECT and RECORD commands due to the following:

- o Analysis of peak activity and long response times is

permitted during extended sessions

- o Data loss is prevented if either the host system or any resource along the session path fails before the session terminates normally

For information on how to synchronize CA NetMaster Network Tracking System (NTS) and Network Error Warning System (NEWS) RTM data collection and CA NetMaster NTS accounting data collection, refer to the CA NetMaster Management for SNA documentation.

6.3.10 Determining Number of Route Element/TG Names

Although the NLDM Route (NVS RTE) File can carry up to nine route element names (RTEELNAX) and nine transmission group names (RTETGNMx) in each observation, the file is shipped with only three route element names (RTEELNA1 - RTEELNA3) and three transmission group names (RTETGNM1 - RTETGNM3) activated to minimize its size. If a significant number of logical unit to logical unit (LU-LU) sessions in your network span more than three route elements or transmission groups, you may wish to increase the number of route element and transmission group names in the NVSRTE file.

A simple way to determine if this increase is necessary is to examine the content of the element Number of Route Elements in Table (RTENRRE). If the value of this element is greater than three for a large number of the virtual routes in your network, you should increase the number of route element and transmission group names in the file.

You can change the number of RTEELNAX and RTETGNMx members in each observation in the NLDM Route File by modifying the RTEELNAX and RTETGNMx statements in the SNTGENIN member in sharedprefix.MICS.GENLIB. Refer to Section 6.2.1.1.2, Adding New Data Elements, in the CA MICS System Modification Guide for complete instructions. In the example below, the number of route element names is increased from three to four by activating Route Element 4 Name. To accomplish this,

- o Modify the name statement for RTEELNA4 in sharedprefix.MICS.GENLIB(SNTGENIN) by replacing each N with 0 in the DETAIL, DAYS, WEEKS, and MONTHS timespans, and
- o Run the component generator for the CA MICS Network Analyzer.

1. RTEELNA4 before the change (inactive in all timespans)

```
TIME-SPAN
X D W M Y
-----
ALIAS RTEELNAX
NAME RTEELNA4    00  N N N N N  Route Element 4 Name
```

2. RTEELNAX after the change (active in DETAIL, DAYS, WEEKS, and MONTHS timespans)

```
TIME-SPAN
```

```

                                X D W M Y
                                -----
ALIAS RTEELNAX
NAME RTEELNA4      00  0 0 0 0 N   Route Element 4 Name

```

Note: Replacing N with 0 in the YEARS timespan would have no effect because the NLDM Route File is not supported in the YEARS timespan. Route Element 4 Name must be activated in the DETAIL timespan if it is to be activated in any of the higher timespans. The value of the RTEELNAX in the higher timespans is derived from its value in the DETAIL timespan.

You should note that NetView does not necessarily record the names of all of the route elements traversed in the route element table. In some cases one or more of the route elements will be defined in the configuration data portion of the SMF type 39 records and will not be restated in the route element table. The CA MICS data element RTENRRE reflects the number of elements defined in the route element table. To know the actual number of route elements traversed, you should refer to the CA MICS data element RTENRTRE, Total Number of Route Elements Traversed.

6.3.11 CA NetSpy Data Considerations

CA NetSpy data will vary depending upon the environment in which it operates and the processing options you have chosen. This section discusses several CA NetSpy options and the effect your choices will have on the data in the CA MICS database. It also discusses a special CA MICS option that will eliminate the inflation of character traffic and connect time in certain multiple session manager environments.

Each issue is discussed in a separate section. The topics are:

- 1 - Multiple Session Manager Considerations
- 2 - Processing Subtype S and U Records
- 3 - Response Distributions and CA NetSpy Options
- 4 - Calculating Total Response Time

6.3.11.1 Multiple Session Manager Considerations

Section 6.8, Multiple Session Manager Considerations, describes the data effects when monitors such as NetView, NPM, and CA NetSpy collect data on user sessions controlled by a multiple session manager such as Tivoli NetView Access. You should carefully review and understand Section 6.8 before proceeding with the explanation below.

CA NetSpy provides a special interface to resolve the data inflation problems present in a multiple session manager environment. This interface resolves these problems only for the CA NetSpy VTAM Interface data (contained in the terminal activity file and application activity file) and not for the CA NetSpy network session accounting/network gateway accounting data (contained in the NCP network accounting file). This interface is implemented through a handshake between the multiple session manager and CA NetSpy whenever a new application session is started or the user at a terminal switches between applications. The result is that the CA NetSpy terminal record, which represents each virtual terminal session between the multiple session manager and the real application, contains valid network response times and identifies, as the Secondary Logical Unit (SLU), the name of the real terminal that initiated the session through the multiple session manager. CA NetSpy also identifies these records as "virtual terminal" records with a flag. In the CA MICS SNTNSS file, a virtual terminal session is indicated when variable NSSVSESS has a value of Y.

CA NetSpy also sets a "multiple session manager" flag in each application record it produces for a multiple session manager. This flag is carried into the appropriate application and terminal records by the CA MICS Network Analyzer Option. The PLUMSMGR flags in the SNTNSS and SNTNSP Files are set to "Y" when the application (PLU) is recognized by CA NetSpy as a multiple session manager.

These flags are useful when you want to summarize data in the SNTNSS File by terminal. Suppose, for example, you want to know the total character traffic, NSSNRBYR plus NSSNRBYS, to terminal T1102015.

The summarization sequence for the SNTNSS File results in an observation for each application (PLU) and terminal (SLU). In the case where a user is logged on to a multiple session manager and has two simultaneous applications (TSO and CICS) active through it, there are three records in the SNTNSS File for each interval of data. If the real terminal name (SLU)

is T1102015, then the records are:

Record 1 - SLU=T1102015, PLU= multiple session manager name

Record 2 - SLU=T1102015, PLU= TSO

Record 3 - SLU=T1102015, PLU= CICS

Record 1 contains character traffic information for all data transferred between the real terminal and the multiple session manager (for example, 47,225 characters).

Records 2 and 3 contain character traffic information for all data transferred between the terminal and each of those applications (for example, 21,225 characters for TSO and 24,100 characters for CICS).

Note that the session between the real terminal and the multiple session manager recorded 1,900 more characters than the total of the other sessions. This is due to interaction between the terminal user and the multiple session manager.

If you merely summarize the file by terminal name, you will get a total character count of 92,550, approximately double the real traffic to the terminal. Instead, you may use either the NSSVSESS or the PLUMSMGR flag to eliminate the records with the redundant information. If you want to preserve the breakdown by application (TSO and CICS), eliminate records with PLUMSMGR=Y. If you are concerned about accurate network traffic statistics, then eliminate the records with NSSVSESS=Y.

An alternative to remembering to process this data as described above is to use the SNTOPS parameter "DELETEDMS YES" to eliminate the records for the session between the multiple session manager and the real terminal as the raw data is being entered into the SNTNSS File. When this parameter is used, only the virtual terminal records will end up in the SNTNSS File. While this eliminates the possibility of redundant data from improper summarization, it has these drawbacks.

- o Virtual terminal session data is missing the user's interaction with the multiple session manager. It therefore may understate the volume of traffic to the terminal.
- o Multiple session manager data compression features actually reduce the amount of data sent to the terminal. Thus, the count of character traffic in the record that is dropped using "DELETEDMS YES" may actually be less than that of the

combined virtual terminal session records. However, the count in the record dropped more accurately reflects the traffic in the network.

6.3.11.2 Processing Subtype S and U Records

Terminal statistics may be recorded in CA NetSpy record subtypes S, T, and U.

You can control which records CA NetSpy produces by defining the CA NetSpy initialization parameters in member INITPRM of the partitioned data set NETSPY.CNTL. Refer to Section 9.3.1 in this guide.

6.3.11.3 Response Distributions and CA NetSpy Options

CA NetSpy provides four response distribution targets which you may associate with either host response time only, or total response time (a combination of host and network response). If you specify the CA NetSpy parameter TARGETS=HOST, then the response distribution fields will be updated whenever a host response is complete, based on the value of ONLY the host response time. If you specify the CA NetSpy parameter TARGETS=USER, then the response distribution fields will be updated not based on combined host and network response times, but ONLY when there is a valid network response to accompany the host response time.

Once CA NetSpy data is in the CA MICS SNTNSS and SNTNSP files, you may determine which option was selected by examining the common variable RDSTTYPE, which is set to 'HOST' or 'USER'. This will tell you whether to associate the response distribution variables (NSSRDST1-5; or NSPRDST1-5) with NSSAVTTM, Average Total Response Time, or NSSAVHTM, Average Host Response Time.

6.3.11.4 Calculating Total Response Time

It is possible that not all response events have network response time measured for them. This will be true if the CA NetSpy FORCEDR (force definite response) option associated with the APPL parameter is valued at less than 100 (100 indicates that 100 percent of all transactions will have the definite response option activated; 80 indicates that only 80 percent of the responses will have definite response activated, etc.). This will also be true if FORCEDR is not used at all, and not all application transactions use definite response.

CA MICS Network Analyzer provides for this in its calculation of total response time and average total response time.

Total network response time is calculated as follows. First, average network response time is calculated as the network response time measured by CA NetSpy divided by the number of network response events. Then, the average network response time is multiplied by the total number of responses. Total number of responses is set to the greater of network and host responses. So, when there are fewer network responses, the CA MICS Network Analyzer simply obtains the average network response and calculates an "approximation" of total network response. The measured network response time is kept in fields NSPNRSTM and NSSNRSTM. The calculated value is maintained in fields NSPCNRTM and NSSCNRTM.

Total response time is calculated as the sum of host response time and "calculated" network response time. The average total response time results from dividing total responses into average total response time.

6.4 Exceptions and NPM Network Parameters

The NPM Network Collection Function has the capability to monitor and record exceptions when specific conditions occur. The data center can set and modify thresholds by which these conditions are recognized using the NETCOLL command.

When exceptions are recognized by NPM, they are recorded in one of the following records:

- o The SMF type 28 subtype x'18' record (monitor exception).
- o The SMF type 28 subtype x'19' record (monitor resolution) if the parameter XRES=YES is specified on the NETCOLL command.

In this case, the exception and resolution records are written only at the first interval when the threshold is exceeded and at the last interval when the resource returns to within bounds. The resolution record contains a count of the number of intervals since the exception and the reason for the resolution.

CA MICS Network Analyzer processes these exception and resolution conditions to create the Network Incident (SNTNIN) File. Exceptions 12181 through 12209 result directly from this data. CA MICS exceptions are described in Chapter 4.

To set or modify the exceptions, their thresholds, the resources for which exceptional conditions are to be monitored, or the interval in which they are recorded, refer to the description of the NETCOLL command in the Tivoli NPM documentation.

6.4.1 Correlating Data Sources to Reports

Each CA MICS Network Analyzer Option report, in tabular or exception form, is built using data from a unique input data source. The product does not attempt to mix data from more than one source in any report.

Figures 6-14 and 6-15, Data Sources and Corresponding SNA Network Reports, show which data sources are necessary for which reports.

Data Source/ Record Description	Record Type	Tabular Report	Exception Report
NPM:			
NPM Network Interval	SMF 28	SNT208	12001-12005
		SNT209	12061-12062
		SNT215	
		SNT216	
		SNT401	12121-12124
NPM Network Monitor Event	SMF 28		12181-12209
NPM Session Data	SMF 28	SNT101	12661-12663
		SNT103	12780-12782
		SNT201	
		SNT203	
		SNT403	

Figure 6-14. Data Sources & Corresponding SNA Network Reports

Data Source/ Record Description	Record Type	Tabular Report	Exception Report
NetView Hardware Monitor or CA NetMaster NEWS	SMF 37	SNT601	12541-12542
		SNT602	12601
NetView Session Monitor	SMF 39	SNT105	12301

or CA NetMaster NTS with		+-----+-----+
3274/3174 RTM		SNT111
		+-----+-----+
		SNT112
		+-----+-----+
		SNT113
		+-----+-----+
		SNT114
		+-----+-----+
		SNT115 12801-12802
+-----+	+-----+	+-----+
NetView Accounting	SMF 39	SNT211 12852-12859
& Availability data		+-----+-----+
or CA NetMaster NTS		SNT212 12862
accounting data		+-----+-----+
		SNT213
		+-----+-----+
		SNT214
+-----+	+-----+	+-----+
CA NetSpy NCP Interface	SMF n	SNT208 12001-12005
(SMF record number is user		+-----+-----+
defined)		SNT209 12061-12062
		SNT215
		SNT216
		+-----+-----+
		SNT401 12121-12124
+-----+	+-----+	+-----+
CA NetSpy VTAM Interface	SMF n	SNT121
(SMF record number is user		+-----+-----+
defined)		SNT122
		+-----+-----+
		SNT221
		+-----+-----+
		SNT222
+-----+	+-----+	+-----+
CA NetSpy General Alerts	SMF n	12181-12195
+-----+	+-----+	+-----+

Figure 6-15. Data Sources & Corresponding Network Reports

6.4.2 NPM Network Parameters Required for Exceptions

The NPM Network collection function has the capability to monitor and record exceptions when specific conditions occur. The data center can set and modify thresholds by which these conditions are recognized using the NETCOLL command. When exceptions are recognized by NPM, they can be recorded in the SMF Type 28 Monitor Event Record, subtype '18'X. Monitor Resolution Records, subtype '19'X, are produced if the parameter XRES=YES is specified on the NETCOLL command. In this case, only at the first interval when the threshold is exceeded and the last interval when the resource returns to within bounds will the exception and resolution records be written. The resolution record contains a count of the number of intervals since the exception and the reason for the resolution.

CA MICS Network Analyzer processes these exception and resolution conditions to create the Network Incident (SNTNIN) File. Exceptions 12181 through 12209 result directly from this data.

To set or modify the exceptions, their thresholds, the resources for which exceptional conditions are to be monitored, or the interval on which they are recorded, refer to the Tivoli NPM documentation.

6.4.3 Creating Performance Classes for Reporting

Control units (3274s and 3174s) with the Response Time Monitor feature installed measure end-user response time for terminal sessions. This unique feature also allows you to specify response time objectives as the percentage of all transactions being less than a predetermined value (in seconds). For example, an installation determines that the terminals attached to control unit XYZ would provide adequate service if 90% of all transactions have end-user response times within three seconds. These objectives are defined to NetView Session Monitor or CA NetMaster NTS and to the control unit. If, during a predefined interval (such as 30 minutes), that objective is not met, the control unit and NetView or CA NetMaster record the objective as missed.

Response objectives relate to NetView performance classes and CA NetMaster RTM classes - both of which are referred to here as performance classes. A performance class constitutes any grouping the installation chooses. For example, all users on the same link may belong to a performance class; or, all TSO users may belong to a performance class. With NetView, the installation defines the performance class service objectives, then maps the terminal sessions to the appropriate performance classes using the NetView MAPSESS definition statement. With CA NetMaster, the Session Class definition provides a similar function to the NetView MAPSESS definition statement.

The following reports are based on installation-defined performance class:

- o Exception Report 12301, Response Objective Missed for Performance Class
- o Tabular Reports
 - SNT105, NLDM Service by Performance Class
 - SNT115, NLDM Service by Performance Class
- o Sample Graphic - Application Response by Performance Class
- o MICF Inquiries
 - SNTCD1, SNTPD1 - NetView Daily Avg Responses by PCLASS
 - SNTCD4, SNTPD4 - NetView Daily % Resp Within Obj by PCLS

For more information on how to establish and control NetView performance classes, refer to the descriptions of the PCLASS and MAPSESS definition statements in the Tivoli NetView documentation. For similar information on CA NetMaster, refer to the descriptions of RTM classes and Session classes in the CA NetMaster Network for SNA documentation.

6.4.4 Adding Tabular Reports to the DAILY Job

The CA MICS Network Analyzer Tabular Reports can be integrated into the DAILY job using the procedure described in Section 3.1.1.3, Integrating Reports into the DAILY CA MICS Job. Once you have defined the reports you wish to run, you may use this procedure to provide daily reports as part of the DAY500 step.

6.5 NPA to File Conversion Utility

This utility is no longer supported by the CA MICS Network Analyzer.

6.6 Basic Network Accounting

Historically, billing for network resources has been largely relegated to the few adventurous organizations that dared to experiment. Now, the information in the CA MICS Network Analyzer and the billing facilities of CA MICS Accounting and Chargeback can be combined to offer a network accounting approach which will satisfy the basic requirements of many enterprises.

Basic network accounting is supported for multiple information sources: CA NetSpy terminal data, CA NetSpy network session accounting data/network gateway accounting data, NetView Performance Monitor (NPM) session data, NPM network session accounting/network gateway accounting data, NetView Session Monitor Response Time Monitor (RTM) data, NetView Session Monitor accounting and availability data, CA NetMaster RTM data, and CA NetMaster accounting data. Since there is an overlap in information provided by these sources, the decision on which source(s) to use is governed by the needs of the enterprise, the specific information available from each source, and the operational costs associated with each network monitor.

Since more than one network monitor can collect data for the same SNA session, it is possible that you will develop a billing scheme that causes duplicate billing for some sessions. For instance, if you are billing for session connect time or characters transmitted based on information from both NPM and NetView, then you may end up billing some users twice for the same session activity. You should carefully evaluate these considerations when constructing a billing scheme based on network monitor data from more than one source.

Billing is supported for connectivity to specific network resources, session duration, and character traffic for terminals or groups of terminals in session with specific applications. A differential charge may be assessed for different classes of service, local or remote attachment, transmission priority, explicit route, virtual route, or any of several other service or configuration related factors.

The following topics are discussed in this section to provide you with an overview of basic network accounting support:

- 1 - Accounting Information Sources
- 2 - Identification of Sessions for Differential Billing

In addition, Section 8.1, CA MICS Accounting and Chargeback Interface, contains a list of billable elements and specific issues you should consider before implementing basic network accounting for your enterprise.

6.6.1 Accounting Information Sources

The basic network accounting approach supported by the CA MICS Network Analyzer and CA MICS Accounting and Chargeback permits the use of data from the following information sources:

- o CA NetSpy Network Session Accounting
- o CA NetSpy Network Gateway Accounting
- o CA NetSpy VTAM Interface: Terminal Activity
- o Network Performance Monitor (NPM) Session
- o NPM Network Session Accounting
- o NPM Network Gateway Accounting
- o NetView Session Monitor Response Time Monitor
- o NetView Session Monitor Accounting and Availability
- o CA NetMaster NTS Response Time Monitor
- o CA NetMaster NTS Accounting

These sources provide different views of the data and permit different ways of performing network accounting. There are six CA MICS Network Analyzer files that contain data from these sources, and which may be used for accounting:

@sntactg

Each of these files is described in Chapter 5, along with a list of the data elements associated with each file. See the CA MICS Data Dictionary for a description of specific data elements and their use within each file. This overview should help you to select the information appropriate to your billing needs.

Each file contains certain basic information:

- o The NCP Network Accounting File (SNTNAC) contains network traffic (messages and characters) and connect time information for terminal sessions collected by the NCP NPALU. Either CA NetSpy or NPM may input network session accounting or network gateway accounting data to this file.
- o The CA NetSpy Terminal (SNTNSS) File contains a variety of information useful for billing purposes including information about the the volume of network traffic, the network session duration, and the response time associated with each monitored SNA session.
- o The NPM User Activity (SNTPSU) File contains network

response and traffic statistics, along with some interesting configuration and service information, such as transmission priority and virtual route number. It does not contain session connect time since the source, NPM Session data, is missing this information.

- o The NLDM Session Accounting (NVSNSA) File contains connect time, message and character traffic (divided into sent/received and control/data categories), and the performance class assigned by the installation as part of NetView implementation. It contains a minimum of configuration information to keep the file size to a reasonable limit. Either NetView or NLDM, or CA NetMaster NTS may be the data source for this file.
- o The NLDM Session Connectivity (NVSNSC) File provides more complete connectivity information than the NVSNSA File, while retaining a minimum of information for billing purposes, including connect time, response events, and total characters transmitted. Also, like the PSU file, it contains several interesting configuration and service elements, such as transmission priority and class of service. Either NetView or NLDM, or CA NetMaster NTS may be the data source for this file.
- o The NLDM Response Time (NVSRTM) File contains only response information, including number of times response objectives were met, number of responses completed within specific objective times, and average response time. Either NetView or NLDM, or CA NetMaster NTS may be the data source for this file.

Section 8.1.3, Network Accounting Considerations, discusses other important issues you should consider before choosing a data source for billing purposes.

6.6.2 Identification of Sessions for Differential Billing

A standard requirement for resource billing is differential charging based on service or configuration.

The user with a locally-attached terminal may be charged a premium versus the user with a remotely-attached device since the locally-attached terminal provides faster response time. Or, based on the additional cost of the facilities for a remotely-attached user, the differential may be applied in exactly the opposite way.

To accommodate this requirement, logical unit-to-logical unit (LU-LU) sessions are distinguished as local, remote, or application-to-application (APPL-APPL) by the CA MICS Network Analyzer Option. Other session types (for example, system services control point to system services control point (SSCP to SSCP)) are designated as "other." Users of the CA MICS Accounting and Chargeback Option may, through a special feature called XMITTYPE, set different rates for each billable element depending upon whether the session is local, remote, or APPL-APPL. For example, the cost for locally-attached devices could be set at \$.04 per thousand characters, while the cost for remotely-attached devices could be set at \$.02 per thousand characters.

The method used by the CA MICS Network Analyzer Option to distinguish local, remote, and APPL-APPL sessions is described in Section 6.7. If you choose this billing approach, be sure to read this section before you finish installing the CA MICS Network Analyzer Option.

In addition to this facility, CA MICS Network Analyzer Option provides for differential billing based on other service and configuration considerations. For example, this capability could be useful for an enterprise that assigns a surcharge to network traffic that receives a higher priority, and therefore faster service. One way to assign different priorities to different types of work in an SNA network is to use transmission priorities. Transmission priorities may be assigned to different classes of work so that, for example, interactive traffic receives a higher priority than batch traffic. Transmission priority values of 0, 1, and 2 can be assigned, with 2 representing the highest priority.

In the example where "interactive" and "batch" are assigned different priorities, the data center may assign "interactive" the highest priority of 2, and "batch" the lowest priority of 0. The enterprise may want to apply a

factor to charges for interactive traffic that result in their cost per thousand characters being 1.5 times the standard cost, which is applied to batch traffic. The way to implement such a billing strategy using the CA MICS Network Analyzer Option is through the Network Service Group facility, described in the following sections.

- 1 - Network Service Group Definitions (NETGROUP)
- 2 - NETGROUP Classification Examples

6.6.2.1 Network Service Group Definitions (NETGROUP)

The CA MICS Network Analyzer supports the data element NETGROUP in each of the six files available for accounting:

- o NCP Network Accounting (SNTNAC) File
- o CA NetSpy Terminal (SNTNSS) File
- o NPM User Activity (SNTPSU) File
- o NLDM Session Accounting (NVSNSA) File
- o NLDM Session Connectivity (NVSNSC) File
- o NLDM Response Time (NVSRTM) File

NETGROUP is used to classify a network session according to its service requirements or its configuration characteristics. The classifications permit differential billing based on service requirements or configuration. For example, an enterprise may want to charge a premium for sessions which receive a high transmission priority. Sessions with a transmission priority greater than 0 could be charged at the rate of 125% of the normal charge for character traffic. All other sessions would be charged at the standard billable rate (that is, 100%).

Defining network service groups is a two-step process. First, each network group is identified by a network group number (an identifying number in the range 1-256), a service factor (a value that identifies the rate at which session charges will be assessed), and a description. This information is recorded in prefix.MICS.PARMS(NETGROUP), described in Section 7.3.6 of this guide. Then a routine is coded to set NETGROUP in the appropriate files so it can be used for network accounting. This routine, called NETGPRT (also a member of prefix.MICS.PARMS), is discussed in Section 7.3.7 of this guide.

6.6.2.2 NETGROUP Classification Examples

Establishing network groups results from the decision to differentially charge for network resources based on expected service or configuration parameters. You may find the examples below useful in your decision-making process.

CLASSIFICATION BY CONFIGURATION

Some network users require specialized facilities to ensure high speed transmission, extended availability through redundant hardware, extremely low error rates, or quick response time. Installing high speed links and transmission groups, assigning high transmission priority to specific classes of work (higher priority for interactive rather than batch transmissions), or providing for redundant communication lines are examples of ways in which high priority users may be provided with better service on a network. As a direct result of the additional cost of these facilities or in recognition of the improved service they afford, the enterprise may wish to charge a premium for this type of service.

The CA MICS Network Analyzer provides data which can be used to distinguish configuration and service differences, such as link name (SLULINK), controller name (SLUPU), virtual route number (e.g., NSCVRTE), transmission priority (e.g., NSCTRPTY), or explicit route (e.g., NSCEXRTE).

CLASSIFICATION BY LOCATION

An enterprise may wish to break the assignment of NETGROUP numbers into blocks, assigning a block of numbers to specific networks. The CA MICS Network Analyzer supports the data element NETWRKID, a user-defined data element you can use to identify individual networks.

CLASSIFICATION BY PERFORMANCE CLASS

CA MICS Network Analyzer supports the NetView concept of performance class as the data element PERFCLSS in the NVSRTE, NVSRM, NVNSA, NVNSC files. The CA NetMaster RTM class is equivalent to the NetView performance class. In this guide, RTM class is referred to as performance class.

Performance classes are defined by each site when NetView or CA NetMaster is installed. PERFCLSS is generally used for classifying or grouping users for reporting response time so that response objectives and distribution thresholds are the same for users who perform similar functions and the response times recorded by the Response Time Monitor may be easily evaluated for each group of users defined to be within the same PERFCLSS.

PERFCLSS may be adapted for use in differential billing so that the charges for one group of users are adjusted to 75 percent of the standard charge assessed for data traffic and connect time to all other users. In this case, a service factor of .75 would be associated with the particular PERFCLSS.

6.7 Identifying Local Vs. Remote Sessions (ffflDEV)

Because most CA MICS Network Analyzer data sources do not identify sessions as local or remote, this information is determined from the data available. The approach taken is to compare primary to secondary subarea identifiers (NPM) and primary and secondary subarea physical unit identifiers (NetView and CA NetMaster). When the identifiers are equal, the session is considered to be a local session. When the identifiers are unequal, the session is considered to be a remote session.

There are two exceptions:

- o To account for logical unit to logical unit (LU-LU) sessions in which the secondary logical unit (SLU) is an application, you can designate a list of applications that can participate in APPL-APPL sessions by coding the application names in prefix.MICS.PARMS(NETAPPL). The CA MICS Network Analyzer identifies any session whose SLU is found in the NETAPPL table as an APPL-APPL session. NETAPPL is described in Section 7.3.8.
- o Sessions that are not LU-LU, such as system services control point to physical unit (SSCP-PU) sessions, are identified as "other" sessions.

The data element ffflDEV (local device flag) is carried in the SNTNAC file (NACLDEV), the SNTPSU file (PSULDEV), the SNTNSS file (NSSLDEV), and the NVSNSC file (NSCLDEV). The local device flag is set to indicate local (L), remote (R), APPL-APPL (A), or other (O).

6.8 Multiple Session Manager Considerations

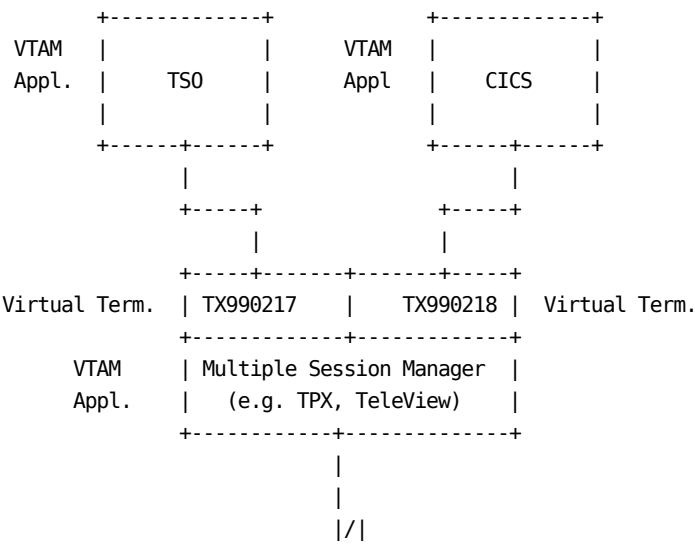
A multiple session manager is a VTAM application that lets a terminal user maintain active sessions with more than one host application simultaneously. The key advantage of such a product is that it eliminates the need for a user who requires access to two or more host applications to log off of one application and log on to the other. This in turn reduces system resources for application LOGONs and enhances end user productivity.

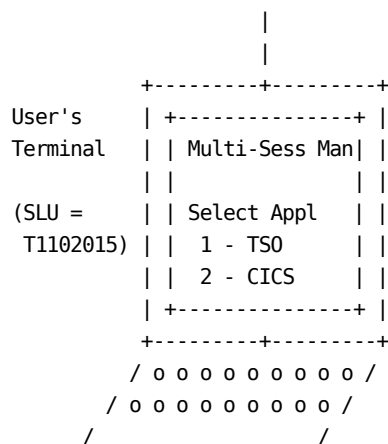
Examples of multiple session managers are the following:

- o CA-TPX,
- o CA-Teleview
- o SOLVE: Access Session Management
- o NetView Access, Tivoli

There are many multiple session manager products on the market today. While each is implemented somewhat differently, there are specific data-related issues that are common among them.

A multiple session manager introduces a separate layer in the interface between the user and the host application. The multiple session manager layer controls the user's access between 16 to 255 separate applications, depending upon the product's implementation. Figure 6-16, Multiple Session Manager User Session, illustrates the interface between the user at a terminal, the multiple session manager, and the host applications.





The terminal user is identified by a userid/password. Once logged on to the multiple session manager, the user can initiate sessions with authorized host applications. In Figure 6-16, the user can log on to TSO and CICS. Once logged on to these applications, the user can switch at will between them without having to log off one before logging on to the other.

To accomplish this, the multiple session manager establishes, in the example illustrated in Figure 6-16, three separate sessions. First, there is a session between the user's terminal and the multiple session manager. Second, a virtual terminal session is established between each real application (TSO and CICS) and a virtual terminal that is associated with the multiple session manager. By VTAM rule, the virtual terminal name must be different from the real terminal name.

Three sessions are established using the example in Figure 6-16:

- ```
o Application = TPX; Real Terminal = T1102015
o Application = TS0; Virtual Terminal = TX990217
o Application = CICS; Virtual Terminal = TX990218
```

## DATA ISSUES

There are several issues that must be considered when evaluating data recorded by products like NetView Session Monitor, NPM Session Subsystem, and CA NetSpy, for users



accessing multiple applications through a multiple session manager.

First, data will be recorded for each real and virtual session established by the multiple session manager. In the example above, each session will be identified by session partners, as follows. PLU is the primary logical unit, or primary session partner (usually an application); SLU is the secondary logical unit, or secondary session partner (often a terminal).

- o TPX session with real terminal

PLU = TPX  
SLU = T1102015

- o Virtual terminal session with TS0

PLU = TS0  
SLU = TX990217

- o Virtual terminal session with CICS

PLU = CICS  
SLU = TX990218

The virtual terminals identified by SLUs TX990217 and TX990218 may bear no relationship to the real terminal, T1102015, if a multiple session manager feature called "pooling" is used. With pooling, virtual terminal names are obtained as needed from a pool of virtual terminal names. The advantage to using this feature is that new real terminals can be added to a system and their users can take advantage of a multiple session manager without requiring an update to either VTAM or tables in the host application. The disadvantage is that there is no way for an analyst or end user of the data produced for such a virtual session to determine what real terminal was in session with the host application. On the other hand, the record that contains data for the real terminal session does not identify the host application (it identifies, instead, the multiple session manager name). Where pooling is not used, data for the virtual terminal session identifies a terminal (SLU) that can be translated to the real terminal (SLU) name, but this must be understood by the analyst or user of the data in order to make a correct interpretation of the information.

Second, network message and character counts and session connect time are included in the data for both the real

terminal session and each of the virtual terminal sessions. The analyst must be careful when combining information from these records because the results will be inflated.

Third, network response times are missing in the virtual terminal session records.

Fourth, performance monitors like Tivoli NPM and CA NetSpy rely on the use of the definite response (DR) feature to calculate network response time. DR is an application option flag, set in the outbound message, which requires the terminal controller to return a positive indication to the application that the message arrived at the terminal. It is frequently used by host applications to synchronize transmission to the terminal. When DR is used, NPM and CA NetSpy can determine network response time as the difference between the arrival time of the DR and the time the message was sent to the terminal (with adjustments to compensate for differences in character counts between the terminal user's input message and the short message that returns as the result of a DR request).

Some multiple session managers do not pass on the definite response flag with the outbound message, but instead return an immediate DR to the host application. When this occurs, network response time is rendered meaningless.

This problem can be overcome if the network monitor provides the facility to activate DR in the VTAM interface, after the multiple session manager has already handled the outbound message. CA NetSpy is an example of a network monitor with such a feature. The CA NetSpy FORCEDR parameter is used to invoke this option.

CA NetSpy also has a multiple session manager interface that can reduce the problems these products normally present in network monitor data. This interface and its effects are described in Section 6.1.4.8, CA NetSpy Data Considerations.

## 6.9 Processing Network Monitor Data From VM Hosts

Both VM CA NetSpy and VM NPM network monitor data can be processed by the CA MICS Network Analyzer Option. Both of these products are capable of producing records in a VM environment that are equivalent to those produced by their z/OS counterparts. It is your responsibility to transport these records to the z/OS host where CA MICS DAILY update processing will occur.

For VM CA NetSpy, you must transport the data contained in the CMS files identified in the LOG1 and LOG2 FILEDEF statements in your NPM/VM startup EXEC.

For VM NPM, you must transport the data contained in the CMS files identified in the FNMLOG1 and FNMLOG2 FILEDEF statements in your NPM/VM startup EXEC.

In addition, you must make minor changes to the INPUTSMF member of prefix.MICS.PARMS to cause the OS file containing your VM CA NetSpy and/or VM NPM data to be concatenated into the SMF input stream for the DAY056 step of your CA MICS DAILY update job. These changes are described in Section 7.6, Product-Specific JCL Information, of this guide. After running a JCLGENU job to regenerate the JCL for your DAILY update job, you will be able process the network monitor data from your VM hosts.

## 6.10 CA MICS and CA SMF Director Interface

CA SMF Director is an SMF management product with special features that can be used to optimize CA MICS processing. CA SMF Director can significantly reduce operational overhead by creating content specific files while simultaneously creating an SMF historical archive during the SMF dump process.

CA MICS DAILY and incremental update operational jobs can be modified to take advantage of this product, provided your site is licensed for and has CA SMF Director installed in your environment.

CA SMF Director provides functions that extract SMF data at dump time or from previously archived SMF files. These functions eliminate the need for any external utilities used for preprocessing of the SMF dump tape for data extraction prior to execution of the DAILY job. In addition, the DAYSMF step of the CA MICS DAILY job may no longer be required. For details on how to eliminate the DAYSMF step, see section 5.10, Removing the DAYSMF Step from the DAILY Job of the PIOM guide.

CA SMF Director SPLIT and EXTRACT statement operands provide a way for you to create content specific files to meet your requirements. The main functions of the operands include the ability to:

- o Select system identifiers
- o Select or exclude SMF record types and subtypes
- o Use conditional statements for granularity
- o Define time boundaries for SMF data

To use the SPLIT function of CA SMF Director for CA MICS components, one or more SPLIT statements must be coded. The split is performed at SMF dump time and the files can then be used as input to products in one or more units. The same results can be accomplished by using the EXTRACT function of CA SMF Director, which retrieves data from the previously created history files. For more information on the SPLIT and EXTRACT functions, see the CA SMF Director User Guide at <http://ca.com/support>.

A complete set of SMF record types and subtypes, for each CA MICS component that inputs SMF data, can be found in `sharedprefix.MICS.PARMS(cccSMFD)`, where `ccc` is the three-character product identifier. Each PARMS member lists the available SMF record types and subtypes for that component in a format suitable for use in CA SMF Director SPLIT and EXTRACT statements. These members are provided as examples only; the CA SMF Director JCL should not reference `sharedprefix.MICS.PARMS(cccSMFD)`.



# Chapter 7: PARAMETERS

---

Defining the product parameters requires that you gain the necessary understanding of your data center and its needs and translate that understanding into CA MICS parameters.

This chapter requests that you:

- o Make several policy decisions
- o Complete various worksheets
- o Translate the worksheet entries into the corresponding CA MICS parameter library entries

These activities represent the major portion of the product installation process.

The CA MICS administrator should use this chapter as a detailed reference when installing or modifying the product in conjunction with the PIOM. Chapters 2 and 3 of the PIOM document the mechanics of the installation process and include checklists that describe each installation step.

If you have any questions, contact Technical Support at <http://ca.com/support>.

This section contains the following topics:

[7.1 Environmental Considerations](#) (see page 1080)

[7.2 Complex-level Parameters](#) (see page 1081)

[7.3 Unit-level Parameters](#) (see page 1097)

## 7.1 Environmental Considerations

Before coding product parameters, you need to know about the MVS environment(s) at your installation. Before you specify parameters for the product:

- o Examine existing user groups, account codes, and job control information used on the system. This information helps you code appropriate values for account codes.
- o Review the default options for the parameters to determine their applicability to your site.
- o Review current CA MICS parameter specifications:
  - Review database unit specifications to determine which unit or units should include SMF data.
  - Review the SYSID parameter to determine whether it correlates to the SMF data. Your site's SYSID definition is located in the prefix.MICS.PARMS data set associated with each database unit.
  - Review the CA MICS ZONE parameter to ensure that it reflects the variations in SMF data. This parameter is located in the prefix.MICS.PARMS data set associated with each database unit.
  - Examine existing accounting standards for other CA MICS products, if applicable, to ensure that CA MICS Accounting and Chargeback aggregates information consistently.

The CA MICS Network Analyzer processes input data from more than one source. All input data is processed by the DAY056 step in the DAILY job as part of the same process. By reviewing the MICSLOG output of the DAY056 step of the DAILY job, you can determine exactly what SMF record types and subtypes were present in the input data stream for each of your MVS or VM hosts.

Following CA MICS standards, if an installation fails to provide input from ANY source, the DAY056 step will fail with a U300 ABEND. When you expect this problem but must run the DAILY job anyway, code SYSPARM=NODATA on the EXEC statement of the DAY056 step to prevent the ABEND.

There is no parameterized provision in CA MICS to cause a



similar ABEND when data from one of the required sources is missing but data from other sources is present. If this might happen at your installation, consider coding the \_USRIHL exit to examine the Input History Log file from the DETAIL timespan at the end of DAILY processing. This routine, and a sample exit which provides this function, are documented in Chapter 10.

## 7.2 Complex-level Parameters

Complex level parameters describe the CA MICS Network Analyzer to the CA MICS system. These parameters are discussed in the following subsections:

- 1 - Analyzer Definition Statements (SNTGENIN)
- 2 - Account Code Definition (SNTACCT)
- 3 - Account Code Exit Routine Definition (SNTACRT)

## 7.2.1 Analyzer Definition Statements (SNTGENIN)

A generation definition statement member is provided for the CA MICS Network Analyzer in `sharedprefix.MICS.GENLIB(SNTGENIN)`. The content of `SNTGENIN` members is described in Chapter 4 of the CA MICS System Modification Guide.

If you process CA NetSpy data, you must update the `INPUTSOURCE` statement. You can enter one or more CA NetSpy SMF record numbers to process in `DAY056`.

Code an `OPTION` statement to specify the types of data you will provide to CA MICS.

`INPUTSOURCE` Statement

-----

- o CA MICS Network Analyzer processes data from IBM TCP/IP Communication Services. The TCP/IP can be configured to generate two SMF record types: 118 and 119. Your data center may generate SMF record type 118 from one system and 119 from another or generate both record types simultaneously from a single system. The `sharedprefix.MICS.GENLIB(SNTGENIN)` member `INPUTSOURCE` statement must specify both record types if your data center needs to process all TCP/IP generated data.
- o The CA MICS Network Analyzer processes data from CA NetSpy. CA NetSpy writes a single SMF record with a user-defined SMF record type ranging from 128 to 255 (decimal).

Your CA NetSpy administrator selects a record type and codes it as "SMF=record number" in the `INITPRM` member in the `NETSPY.CNTL` library. The default for this parameter is `SMF=0`, which prevents CA NetSpy from recording SMF data, so your CA NetSpy administrator must explicitly specify this value to effect SMF recording.

If your data center has defined multiple CA NetSpy SMF record numbers, then you must specify all of those numbers on the `INPUTSOURCE` statement in `sharedprefix.MICS.GENLIB(SNTGENIN)`. Select only those CA NetSpy SMF record numbers that you want to process with `DAY056`.

Submit `sharedprefix.MICS.CNTL(SNTCGEN)`. After the `SNTCGEN` completes successfully, edit `prefix.MICS.PARMS(JCLGENU)` so

that it contains no keywords (becomes a blank member) and then submit prefix.MICS.CNTL(JCLGENU).

#### OPTION Statement

-----

The OPTION statement indicates which groups of data elements are going to be kept in the database.

The valid keywords are:

|                 |                                    |
|-----------------|------------------------------------|
| NTRI/NONTRI     | - Network Token Ring Interface     |
| SESMGR/NOSESMGR | - Session Manager                  |
| TIC3/NOTIC3     | - Token Ring Interface Coupler     |
| X25/NOX25       | - X.25 Network                     |
| FRLY/NOFRLY     | - Frame Relay                      |
| TCP/NOTCP       | - Transport Communication Protocol |

You must specify one keyword from each pair. The keywords can be specified in any order and must be separated by one or more blanks.

### 7.2.2 Account Code Definition (SNTACCT)

This section explains how to define the CA MICS Network Analyzer Option account code structure. These definitions apply to every unit database in the database complex.

In CA MICS, data is stored by account number in the following files:

- o NCP Network Accounting (SNTNAC) File
- o CA NetSpy Terminal (SNTNSS) File
- o NPM User Activity (SNTPSU) File
- o NLDM Session Accounting (NVSNSA) File
- o NLDM Session Connectivity (NVSNSC) File
- o NLDM Response Time (NVSRTM) File
  
- o NLDM Route (NVS RTE) File

The NLDM files listed above accept data from NetView Session Monitor/NLDM and from CA NetMaster Network Management NTS.

The parameters that you specify in `sharedprefix.MICS.PARMS(SNTACCT)` define the number of accounting fields that will be carried in these files, the length of each field, and the descriptive names that are associated with each field. Note that once you have defined these fields, you must provide a routine that assigns them values (the SNTACRT member).

First you must determine what your accounting structure will be; then decide how you want it expressed in the database. You can choose to use a different account structure for each file.

Once you design your accounting structure, you must determine the number of accounting fields you will need (CA MICS supports from 1 to 9) and what data will be placed in them. Because the accounting fields are part of the sort sequence, there will be at least one record for each unique combination of values. You must decide between keeping a fine level of granularity via the accounting fields and, therefore, having a large database, or keeping a coarser level of granularity, but perhaps not meeting your reporting or analysis requirements.

While you may assign different values to the accounting fields for each file, the number of accounting fields is not variable and, therefore, must be large enough to accommodate both. In addition, we recommend that you establish an

additional accounting field for future expansion. Thus, if you determine the need for accounting fields 1-4, add SNTACT5.

Three commonly-used choices for setting this account code structure are:

1 - Organization by virtual route

Each record in a summarized timespan represents the activity and response time for a unique combination of PLU, virtual route, transmission priority, and explicit routes (one inbound and one outbound) during the recording interval. This file organization is useful for virtual route planning.

A sample account code structure for this arrangement is shown below:

SNTPSU File

-----

SNTACT1 - PLU  
SNTACT2 - SLUSAPU  
SNTACT3 - VR  
SNTACT4 - TP  
SNTACT5 - Inbound ER  
SNTACT6 - Outbound ER

SNTNSS File

-----

SNTACT1 - PLU  
SNTACT2 - NSSTSA (the terminal subarea number)  
SNTACT3 - NSSVRRTE

NVSNSA, NVNSNC, NVSRTE, NVSRTE Files

-----

SNTACT1 - PLU  
SNTACT2 - SLUSAPU  
SNTACT3 - VR  
SNTACT4 - TP  
SNTACT5 - Inbound ER  
SNTACT6 - Outbound ER

Note: This structure is the same as that described for the SNTPSU file above.

Virtual route numbers are not unique within a network and must be identified by their end-point nodes, PLUSAPU

and SLUSAPU, and transmission priority. PLUSAPU is not included in the account code structure shown above because all CA MICS Network Analyzer Option files have SYSID as a fixed key, which usually corresponds to the PLUSAPU. An exception is an application-to-application session, in which case SYSID corresponds to the SLUSAPU in the host containing the SLU, and it corresponds to the PLUSAPU in the host containing the PLU.

### 2 - Organization by Cluster Controller

Each record in a summarized timespan represents the activity and response time for a controller during the recording interval. A sample account code structure for arrangement by cluster controller is shown below:

SNTPSU File  
(NPM)

-----

SNTACT1 - PLUSAPU  
SNTACT2 - PLU  
SNTACT3 - SLULINK  
SNTACT4 - SLUPU

Note: This organization is not recommended for the NPM SNTPSU file, because it is redundant with the fixed key structure of the NPM Link Activity File, SNTNPL.

SNTNAC File  
(CA NetSpy)

-----

SNTACT1 - PLUSA  
SNTACT2 - PLU  
SNTACT3 - SLULINK  
SNTACT4 - SLUPU

SNTNAC File  
(NPM)

-----

SNTACT1 - PLUSAPU  
SNTACT2 - PLU  
SNTACT3 - SLULINK  
SNTACT4 - SLUPU

SNTNSS File

-----

SNTACT1 - PLU  
SNTACT2 - NSSTSA (the terminal subarea number)  
SNTACT3 - SLULINK  
SNTACT4 - SLUPU

NVSNSA, NVSNSC, NVSRTE, NVSRM Files

-----

SNTACT1 - PLUSAPU  
SNTACT2 - PLU

SNTACT3 - SLULINK  
SNTACT4 - SLUPU

### 3 - Organization by Terminal

Each record in a summarized timespan represents the activity and response time for a terminal during the recording interval. A sample account code structure for this arrangement is shown below:

#### SNTPSU File

-----

SNTACT1 - PLUSAPU  
SNTACT2 - PLU  
SNTACT3 - SLUNETID  
SNTACT4 - SLUPU  
SNTACT5 - SLUSAPU  
SNTACT6 - SLU

#### SNTNAC File (CA NetSpy)

-----

SNTACT1 - PLUSA  
SNTACT2 - PLU  
SNTACT3 - SLUNETID  
SNTACT4 - SLUPU  
SNTACT5 - SLUSA  
SNTACT6 - SLU

#### SNTNAC File (NPM)

-----

SNTACT1 - PLUSAPU  
SNTACT2 - PLU  
SNTACT3 - SLUNETID  
SNTACT4 - SLUPU  
SNTACT5 - SLUSAPU  
SNTACT6 - SLU

#### SNTNSS File

-----

SNTACT1 - PLU  
SNTACT2 - NSSTSA (the terminal subarea number)  
SNTACT3 - SLUPU  
SNTACT4 - SLU

#### NVSNSA, NVSNSC, NVSRTE, NVSRM Files

-----

SNTACT1 - PLUSAPU  
SNTACT2 - PLU  
SNTACT3 - SLUPU  
SNTACT4 - SLUSAPU  
SNTACT5 - SLU

You may establish a different account code structure for NPM, CA NetSpy, NetView, or CA NetMaster. See Section 7.2, Account Code Exit Routine Definition (SNTACRT), for specific

information.

CA MICS Network Analyzer Option accounting fields have names in the form SNTACTn, where n is the sequential number of the accounting field. If three fields are defined, they will be SNTACT1, SNTACT2, and SNTACT3. In your accounting structure, these might identify primary logical unit (application), link (line), and physical unit (3274 cluster controller), respectively. The sequential number is called the account-code level number. There is a maximum of nine levels. A sample account code structure is provided in `sharedprefix.MICS.HOLD.PARMS(SNTACCT)`.

### Coding the Account Code Parameter

-----

The format of the statement is:

level (mask) length description

where:

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| level       | The sort sequence designation of the account code. Up to nine levels may be specified. Level 1 is the highest level and level 9 is the lowest in sort order.                                                                                                                                                                                                                                                                        |
| (mask)      | An option for deactivating account code levels in the DAYS, WEEKS, MONTHS, and YEARS timespans. For example, the DETAIL timespan may use account code levels 1, 2, and 3, while the MONTHS timespan may use only level 1. Setting account code levels by timespan is accomplished by specifying this additional parameter on the account code statements, using values Y or N to specify whether or not the account code is active. |
| length      | The field length of the specified element. Valid lengths range from 1 to 30.                                                                                                                                                                                                                                                                                                                                                        |
| description | The title that describes the account code level. Valid descriptions range from 1 to 40 characters.                                                                                                                                                                                                                                                                                                                                  |

Use the worksheet in Figure 7-1 to collect the information for coding into `sharedprefix.MICS.PARMS(SNTACCT)`. Observe the following conventions when coding:

- o Blank statements are permitted. Comments are coded by



beginning the statement with an asterisk (\*).

- o Account levels must be specified in ascending order, starting with 1. You can specify up to nine account levels, with no gaps between the numbers.
- o The statements are free-form but positional.

#### Additional Notes on Specifying the TimeSpan Mask Option

-----

The timespan mask option is used to deactivate the account code in specified timespans. Specifying a timespan mask requires coding the account code statement using the timespan mask parameter T(.....), as follows:

level T(.....) length 'descriptive title'

This example shows the placement and syntax of the timespan mask on the account code statement. Each "." position in the parentheses represents a timespan in the following order: DETAIL, DAYS, WEEKS, MONTHS, YEARS, and TABLES. For each timespan, a Y indicates that the account level should be active and an N indicates that the account level should be inactive.

This parameter is optional. If it is not coded, the assumed value is T(YYYYYY).

The following rules apply if you code this parameter:

- o DETAIL must always be Y. Account codes may not be deactivated in this timespan.
- o If DAYS is N, then WEEKS, MONTHS, and YEARS must also be N. If the account code level is inactive in the DAYS timespan, it cannot be active in higher timespans.
- o If MONTHS is N, then YEARS must be N. If the account code level is inactive in the MONTHS timespan, it cannot be active in the YEARS timespan.

#### Example

-----

A sample SNTACCT member is illustrated below:

```
* SAMPLE NETWORK ACCOUNTING ROUTINE
 1 8 'PRIMARY LOGICAL UNIT (PLU)'
 2 8 'SLUSAPU NETV/NPM1.3, SLUSA NPM1.2 OR NSPY'
```

```

3 8 'SLUPU IF NLDM OR NETSPY, SLU IF NPM'
4 8 'PERFCLSS IF NLDM, NPM BLANK, NSPY SLU'
5 8 'NOT USED'

```

As you plan for the definition of the CA MICS Network Analyzer Option accounting fields at your data center, be aware that some of the standard reports provided with the product depend on a particular definition of these account codes. Specifically, the SNT113 report assumes that the SNTACT3 element is set to the value of the SLUPU data element for network data from either NetView or CA NetMaster. Similarly, the SNT115 report assumes that the SNTACT4 element is set to the value of the PERFLSS data element for network data from either NetView or CA NetMaster. These are the default settings that were defined when the product was shipped to you.

[illegible]

```
+-----+
| ...5...10...15...20...25...30...35...40...45...50...55...60...65...70.. |
+-----+
```

Figure 7-1. Network Analyzer Account Code Level Definition Worksheet

### 7.2.3 Account Code Exit Routine Definition (SNTACRT)

This section explains how to code an account code exit for the CA MICS Network Analyzer. These definitions will be used for every database unit that contains this analyzer.

A network account code exit routine is a user-written routine that is invoked for each input record processed. This SAS routine builds the account code data elements defined in the previous section. For example, if `sharedprefix.MICS.PARMS(SNTACCT)` defines four account code levels, this user routine builds the data values of those four fields for each record processed.

The object of the account code exit routine definition process is to build the data elements SNTACT1 to SNTACT9 (as many as have been defined in SNTACCT) from the data made available in the DETAIL timespan files. You should follow the exit coding guidelines given in Section 2.3.1.5, Notes on Coding CA MICS Parameters, in the PIOM.

The user account code exit routine is written in SAS code. The testing and accuracy of the process is your responsibility. However, CA MICS provides a sample account code exit routine and certain program aids to help verify the accuracy of the user modifications to the routine. The sample routine is contained in `sharedprefix.MICS.HOLD.PARMS(SNTACRT)`. The worksheet for structuring the network account code exit routine is shown in Figure 7-2.

The account code exit routine has been made available for each of the data elements contained in each of the files for which account fields may be set. The files are:

- o NCP Network Accounting (SNTNAC) File
- o CA NetSpy Terminal (SNTNSS) File
- o NPM User Activity (SNTPSU) File
- o NLDM Session Accounting (NVSNSA) File
- o NLDM Session Connectivity (NVSNSC) File
- o NLDM Response Time (NVSRTM) File
  
- o NLDM Route (NVS RTE) File

The NLDM files accept data from NetView Session Monitor/NLDM and CA NetMaster NTS.

Chapter 5 lists the elements available in each file.

Common elements that might be useful for account codes are:

- PLU - The primary logical unit (application) name
- SLULINK - The name of the link associated with a secondary logical unit
- SLUPU - The name of the SNA physical unit (cluster controller) associated with the secondary logical unit
- SLU - The secondary logical unit (terminal) name

Additional elements that may be useful in the SNTPSU File are:

For NPM

-----

- PLUSAPU - The primary logical unit subarea physical unit
- SLUSAPU - The secondary logical unit subarea physical unit
- PLUNETID - The PLU network identifier
- SLUNETID - The SLU network identifier

In the SNTNSS File, the NSSTSA data element contains the terminal subarea number and can be useful for identifying groups of users at a subarea level.

Elements that may be useful in the NVSNSA, NVNSNC, NVSRTE, and NVSRM Files are:

- PLUSAPU - The primary logical unit subarea physical unit
- SLUSAPU - The secondary logical unit subarea physical unit

The example below assumes that a data center defined five account code levels in SNTACCT, and they are derived as described below:

- SNTACT1 - The host application name (primary logical unit)
- SNTACT2 - If NLDM, CA NetMaster NTS, NPM, the primary logical unit, subarea physical unit name
  - If CA NetSpy, the primary logical unit subarea name
- SNTACT3 - If CA NetSpy, NLDM, or CA NetMaster NTS, the secondary logical unit physical unit name (cluster controller)
  - If NPM, the secondary logical unit name (terminal)
- SNTACT4 - If NLDM or CA NetMaster NTS, the performance

```
class
- If NPM SNTPSU file, blank
- If CA NetSpy or SNTNAC file, the terminal ID
```

SNTACT5 - Blank for future expansion

The COMPT data element specified in the following example is an eight-character product and data source identifier used as a work element during CA MICS DAILY processing. The valid values for this element are:

'SNT NPDA' - NetView (NPDA) or CA NetMaster NEWS SMF record type 37

'SNT NPMN' - NPM Network data SMF record type 28

'SNT NPMS' - NPM Session data or Network Session Accounting data SMF record type 28

'SNT NLDM' - NetView (NLDM) or CA NetMaster NTS SMF record type 39

'SNT NSPY' - CA NetSpy user-defined SMF record type that includes data from CA NetSpy VTAM Interface, NCP Interface, and Network Session Accounting

'SNT TCP ' - IBM TCP/IP SMF record types 118 or 119

WARNING! In the example below, the variable FILEID is used instead of COMPT to set account codes for the SNTNAC file. This is the only file for which account codes may be set based on the value of FILEID. Using FILEID to set account codes for any file other than SNTNAC will cause the SNTACRT exit routine to fail. FILEID was used to assign account codes for the SNTNAC file, because both the SNTPSU file and the SNTNAC file have the same COMPT value (NPMS), and we wanted to set account code values differently for the two files.

Assuming the sample SNTACCT routine described earlier, the SAS code defined for the SNTACRT user account code exit would be:

```
*EXAMPLE - SNT ACCOUNT CODE DERIVATION EXIT
* NOTE: THIS ROUTINE IS %INCLUDED MULTIPLE TIMES SO
* LABELS ARE NOT PERMITTED.
*
* IN THIS EXAMPLE, SNTACT1 = PLU
* SNTACT2 = SLUSAPU/SLUSA
```

```

* SNTACT3 = SLUPU/SLU
* SNTACT4 = PERFCLSS/'BLANKS'/SLU
* SNTACT5 = 'BLANKS'
;

* SET DEFAULT VALUES ;
 SNTACT1 = 'OVERHEAD';
 SNTACT2 = ' ';
 SNTACT3 = ' ';
 SNTACT4 = ' ';
 SNTACT5 = ' ';
* CHECK INPUT DATA SOURCE AND SET ACCOUNT FIELDS ;
 IF COMPT='SNT NLDM' THEN DO; /*NETVIEW, NETMASTER*/
 SNTACT1 = PLU;
 SNTACT2 = SLUSAPU;
 SNTACT3 = SLUPU;
 SNTACT4 = PERFCLSS;
 SNTACT5 = ' ';
 END;
 IF COMPT='SNT NPMS' THEN DO; /* NPM*/
 SNTACT1 = PLU;
 IF NPMVRL GE '0013' THEN SNTACT2 = SLUSAPU;
 ELSE SNTACT2 = SLUSA;
 SNTACT3 = SLU;
 SNTACT4 = ' ';
 SNTACT5 = ' ';
 END;
 IF COMPT='SNT NSPY' THEN DO; /*NETSPY*/
 SNTACT1 = PLU;
 SNTACT2 = NSSTSA; /* SAME AS SLUSA */
 SNTACT3 = SLUPU;
 SNTACT4 = SLU;
 SNTACT5 = ' ';
 END;
 IF COMPT='SNT NPMS' AND FILEID='SNTNAC' THEN DO;
 SNTACT1 = PLU;
 SNTACT2 = SLUSAPU;
 SNTACT3 = SLUPU;
 SNTACT4 = SLU;
 SNTACT5 = ' ';
 END;
END;

```

```

+-----+
| DATA CENTER PREPARATION WORKSHEET: Network Account Code Exit |
| PARMs Library Member is SNTACRT |
| Reference Section: 7.2.3, CA MICS Network Analyzer Option |
+-----+
| |

```

```

| * VALIDATE FOR VALID ACCOUNT CODES, WHERE POSSIBLE ;
|
| IF { account data is valid } THEN DO;
|
| * BUILD ACCOUNT CODE FIELDS AS IN THE WORKSHEET 7-1
|
| SNTACT1=field source 1 ;
| SNTACTn=field source n ;
|
END;
ELSE DO;
* ROUTINE TO BUILD INSTALLATION OVERHEAD ACCOUNT CODES ;
SNTACT1='overhead category' ;
SNTACTn='overhead category' ;
END;
+-----+
...5...10...15...20...25...30...35...40...45...50...55...60...65...70..
+-----+

```

Figure 7-2. Network Account Code Routine Definition Worksheet



## 7.3 Unit-level Parameters

Unit-level parameters control CA MICS Network Analyzer processing. These parameters are stored in the prefix.MICS.PARMS library associated with each database unit you define. The parameters are incorporated into the CA MICS system by the parameter generation process (SNTPGEN).

Note: You must run the generation processes for these options to take effect.

Figure 7-3 identifies each of the system code generation processes for the CA MICS Network Analyzer, their PARMS member inputs, the output MACROs (a member can contain the definition of more than one SAS MACRO) and FORMATS that they generate. The output libraries are at the database unit-level (prefix) unless otherwise noted.

The CA MICS Network Analyzer Options member (SNTOPS) is read by the Parameter Generation Routine (SNTPGEN). SNTPGEN builds the master macros and stores them in prefix.MICS.USER.SOURCE(#SNTMSTR).

Figure 7-3 identifies the MACROs and FORMATS generated during the SNTPGEN process.

| System<br>Code<br>Generator | CA MICS.PARMS<br>Input<br>Member | USER.SOURCE<br>Output Members and<br>SAS MACRO Names                                                                                                                                         | MUOLIB<br>Output<br>SAS FORMATS                                                                                 |
|-----------------------------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| SNTPGEN                     | SNTOPS                           | #SNTMSTR &NSPYSW<br>&NLDMSW<br>&NPDAW<br>&NPMNSW<br>&NPMSSW<br>&NPMVSW<br>&NLDMSW<br>&TCPSW<br>&NACSLMIT<br>&NSCCLMIT<br>&TCPSLMIT<br>&TAPEAPII<br>&ALLSMF<br>&TCPSMF<br>TAPEAPI<br>TAPEAPIO | \$EVTRTYP<br>\$GENEVCD<br>\$NPDAEVC<br>\$SPCEVCD<br>\$NETAPPL<br>\$NETAPPL<br>\$SNTPARM<br>\$TCPSMF<br>\$SNTSYS |

Figure 7-3. SNTPGEN Code Generator Cross-Reference List

The sections that follow show you how to specify the operational parameters that control how input data is processed by the CA MICS Network Analyzer. The names in parentheses are the member names within the prefix.MICS.PARMS data set that contain the parameters described in the section:

- 1 - Processing Options (SNTOPS)
- 2 - INPUTRDR and INPUTSNT PARMS Members
- 3 - JCL Option Definitions (JCLDEF)
- 4 - Network Identifier Exit (SNTNIDRT)
- 5 - Link TP Circuit ID Exit (SNTCIDRT)
- 6 - Network Service Group Definition (NETGROUP)
- 7 - Network Service Group Exit Routine (NETGPRT)
- 8 - Network Application Table (NETAPPL)
- 9 - PLU Identification Routine (SNTPLURT)
- 10 - Database Space Modeling (DBMODEL)

### 7.3.1 Processing Options (SNTOPS)

This section shows you how to specify the operational statements that control CA MICS Network Analyzer processing.

Operational statements are stored in the prefix.MICS.PARMS cccOPS member, where ccc is the component identifier, and are incorporated into the CA MICS system by running the prefix.MICS.CNTL(cccPGEN) job.

```

*
* NOTE: CHANGES to prefix.MICS.PARMS(cccOPS) members
* REQUIRE EXECUTION of prefix.MICS.CNTL(cccPGEN)
* to take effect.
*
* In addition, any change to parameters that
* impact the DAILY operational job JCL such as,
*
* o changing RESTART NO to RESTART YES,
*
* o WORK parameter changes when RESTART NO is in
* effect,
*
* o Specifying TAPEfff (if this product supports
* a DETAIL level TAPE option),
*
* o or changes to prefix.MICS.PARMS(INPUTccc),
*
* will require regeneration of the DAILY job by
* executing prefix.MICS.CNTL(JCLGEN) or by
* specifying DAILY in prefix.MICS.PARMS(JCLGEN)
* and executing prefix.MICS.CNTL(JCLGEN).
*
* Refer to the checklist (if provided) for updating
* cccOPS parameters and running required generation
* jobs.

```

The SNTOPS member contains the following statements, described in detail below. A worksheet for recording the statement values for SNTOPS is shown in Figure 7-4.

#### Required Statements

-----

```
NETWORK ID
ORGSYSID
```

TIME OFFSET or DEFAULT TIME OFFSET  
DATA SOURCES or DEFAULT DATA SOURCES

#### Optional Statements

-----

SNTNAC SUSPEND  
NVSNSC SUSPEND  
TCP SUSPEND  
IBMTCP SMF or DEFAULT IBMTCP SMF  
NETSPY SMF or DEFAULT NETSPY SMF  
NETTCP SMF or DEFAULT NETTCP SMF  
DELETEMs or DEFAULT DELETEMs  
WORK  
MULTWORK/NOMULT  
RESTART  
INCRUPDATE

Unless otherwise specified, the following are general rules for coding all statements above:

- o Blank statements are permitted. Code comments by beginning the statement with an asterisk (\*).
- o The SNTNAC, NVSNSC, TCP suspend keywords are global and may be specified anywhere within the SNTOPS member. Since the keywords are global, they should be specified only once. If they are specified more than once, the last specification will be used as the suspend limit. If they are not specified at all, the default is 30.
- o The WORK, MULTWORK/NOMULT, RESTART, and INCRUPDATE keywords are also global, may be specified anywhere within the SNTOPS member, and should be specified only once. If they are specified more than once, the last specification will be used.
- o The NETWORK ID parameter must be the first parameter defined in the ORGSYSID group.
- o Only one NETWORK ID parameter is required (even for multiple ORGSYSID parameters).
- o You must code the options in the order indicated on the worksheet shown in Figure 7-4.
- o Required statements associated with each ORGSYSID are:
  - TIME OFFSET

- DATA SOURCES

- o The DEFAULT IBMTCP SMF, DEFAULT NETSPY SMF, and DEFAULT NETTCP SMF statements are coded after the first NETWORK ID statement and before the first ORGSYSID statement.
- o The IBMTCP SMF, NETSPY SMF, or NETTCP SMF statement is required when, respectively, NSPY, NTCB, or TCP is coded with a DATA SOURCES statement, and one of the following is true:
  - The DEFAULT IBMTCP SMF, DEFAULT NETSPY SMF, and DEFAULT NETTCP SMF statement is not defined.
  - The DEFAULT IBMTCP SMF, DEFAULT NETSPY SMF, and DEFAULT NETTCP SMF statement is defined but you need to override the default for a particular ORGSYSID.

A sample SNTOPS member describing input from a multiple domain network with three host processors in different time zones is shown below. The three network monitor hosts are Q033, P168, and XTRA. Note that CA NetSpy data is being processed from XTRA and that the session records between terminals and the multiple session manager are to be dropped.

- \* SAMPLE CA MICS NETWORK ANALYZER OPTIONS

```
SNTNAC SUSPEND 15
NVSNSC SUSPEND 15
NETWORK ID NETWORK1
 DEFAULT NETSPY SMF = 132
 DEFAULT NETTCP SMF = 132
 DEFAULT IBMTCP SMF = 118
 ORGSYSID Q033
 TIME OFFSET 0
 DATA SOURCES NLDM NPDA NPMN NPMS NPMV NTRI TCP
 IBMTCP SMF = 119
 ORGSYSID P168
 TIME OFFSET 2
 DATA SOURCES NPDA NPMN NPMS NPMV NTRI X25 NTCB
 NETTCP SMF = 144
 ORGSYSID XTRA
 TIME OFFSET -1
 DATA SOURCES NLDM NPDA NSPY TIC3 X25 TCP
 NETSPY SMF = 183
 DELETEM YES
```

### 7.3.1.1 SNTNAC Suspend Statement

The optional SNTNAC Suspend statement provides suspend processing for the SNTNAC file. CA NetSpy and NPM provide network session accounting (NSA) and network gateway accounting (NGA) data used to build the SNTNAC file. Since sessions can span multiple days, it is necessary to retain the last observation for each session that has not ended, and include that information for processing with the next group of data read. By doing so, the file elements can be correctly calculated for long-running sessions or those that span multiple input data files.

If the SNTNAC Suspend statement is not specified, the default value is 30.

The SNTNAC Suspend Statement has the following format:

SNTNAC Suspend n

where n is a number between 1 and 365. This will identify the number of times information pertaining to a session that has not yet ended will be suspended on the NCP Network Accounting Suspend File (SNTNA1).

### 7.3.1.2 NVSNSC Suspend Statement

The optional NVSNSC Suspend statement provides suspend processing for the NVSNSC file. NetView and CA NetMaster provide Session Monitor data used to build the NVSNSC file. Since sessions can span multiple days, it is necessary to retain the last observation for each session that has not ended and include that information for processing with the next group of data read. By doing so, the file elements can be correctly calculated for long-running sessions or those that span multiple input data files.

If the NVSNSC Suspend statement is not specified, the default value is 30.

The NVSNSC Suspend Statement has the following format:

NVSNSC Suspend n

where n is a number between 1 and 365. This will identify the number of times that information pertaining to a session that has not ended yet will be suspended on the Session Connectivity Suspend File (NVSNS1).

### 7.3.1.3 TCP Suspend Statement

The optional TCP Suspend statement provides suspend processing for the TCPSAP and TCPTSS files. TCP/IP Telnet Server data is used to build the TCPTSS file. Since sessions can span multiple days, it is necessary to retain the last observation for each session that has not ended and include that information for processing with the next group of data read. By doing so, the file elements can be correctly calculated for long-running sessions or those that span multiple input data files.

API Calls for Sockets data is used to build the TCPSAP file. A record is logged either for API Call to start a Telnet session or for any time an FTP command is used. It is, therefore, necessary to retain the last observation for each API INIT action that has not TERMINATED and include that information for processing with the next group of data read. By doing so, the file elements can be correctly calculated for long-running sessions or those that span multiple input data files.

If the TCP Suspend statement is not specified, the default value is 30.

The TCP Suspend Statement has the following format:

TCP Suspend n

where n is a number between 1 and 365 that identifies the number of times that information pertaining to a TCP/IP activity that has not yet ended will be suspended.

### 7.3.1.4 Network ID Statement

The Network ID Statement is required and has the following format:

NETWORK ID networkname

where networkname is a user-specified name that identifies data from a single or multiple domain network.

Each network in a multiple network or SNI (SNA Network Interconnection) network must have its own NETWORK ID. This name must match the value that results from the invocation of the SNTNIDRT exit described later in this chapter.



### 7.3.1.5 ORGSYSID Statement

The ORGSYSID Statement is required and has the following format:

```
ORGSYSID orgsysid
```

where orgsysid is the original system identifier found in the SMF records or a ???? literal string. The Original System identifier must match one of the Original System Identification (ORGSYSID) parameters specified in prefix.MICS.PARMS(SYSID).

A ???? parameter value for the ORGSYSID keyword is a way to direct DAY056 to accept SMF data from original systems that are not explicitly defined. The identifiers of those original systems must still be in prefix.MICS.PARMS(SYSID).

For more information on SYSID, refer to Chapter 2 in the PIOM.

### 7.3.1.6 TIME OFFSET and DEFAULT TIME OFFSET Statements

#### TIME OFFSET

-----

This statement is required if no default is specified. It enables you to combine data from multiple time zones into the same CA MICS database unit.

This can be accomplished by adjusting the timestamps recorded on the CA MICS database to local time. First, select one of the time zones as the base and assign it a TIME OFFSET of 0. Set the TIME OFFSET for each system in a different time zone from the base, according to whether the time zone is east or west of the base system:

- o For a time zone that is west of the base, use a positive number.
- o For a time zone that is east of the base, use a negative number.

TIME OFFSET has the following format:

TIME OFFSET n

where n is the number of hours to be added to or subtracted from the SMF record timestamp and can range from -12 to 12. Specify 0 for data that does not require adjustment.

For example, a user's hub system is located in New York. A satellite system is located in Chicago. The time zone difference is one hour. The following TIME OFFSET specifications are used:

- o New York - TIME OFFSET 0
- o Chicago - TIME OFFSET 1

#### DEFAULT TIME OFFSET

-----

This statement is optional and enables you to define a default value for every implicit/explicit ORGSYSID defined within the network. If the TIME OFFSET is explicitly defined, it will override the DEFAULT TIME OFFSET statement.

The DEFAULT TIME OFFSET statement has the following format:

DEFAULT TIME OFFSET n

where  $n$  is the number of hours to be added to or subtracted from the SMF record timestamp and can range from -12 to 12. Specify 0 for data that does not require adjustment.

### 7.3.1.7 DATA SOURCES and DEFAULT DATA SOURCES Statements

#### DATA SOURCES

-----

This statement is required if no default is specified. It defines the data sources you must supply to CA MICS Network Analyzer for each network and system. The valid values are:

- NSPY - CA NetSpy data
- NTRI - Network Token Ring Interface data from CA NetSpy or NPM
- TIC3 - Token Interface Coupler type-3 data from CA NetSpy or NPM
- X25 - NCP Packet Switching data from CA NetSpy or NPM
- NPDA - NetView Hardware Monitor/NPDA
- GENA/LAN - NetView Hardware Monitor Generic Alert/LAN. If you specify GENA/LAN but do not specify NPDA, then NPDA is automatically included as a data source.
- NLDM - NetView Session Monitor/NLDM
- NPMN - NPM Network data
- NPMS - NPM Session data or NPM network session accounting/network gateway accounting
- NPMV - NPM VTAM data
- NTS - CA NetMaster for SNA, Network Tracking System (NTS)
- NEWS - CA NetMaster for SNA, Network Error Warning System (NEWS)
- NTCP - CA NetMaster for TCP/IP
- FRLY - Frame Relay
- TCP - IBM Transport Communication Protocol/Internet Protocol

The DATA SOURCES statement has the following format:

DATA SOURCES - datasource1 datasource2 datasourcen

where datasourcen is a value taken from the list above.

#### DEFAULT DATA SOURCES

-----

This statement is optional. It is a default value for DATA SOURCES. The options defined with this keyword apply to every implicit/explicit ORGSYSID defined within the network, although they can be overridden by explicitly coding DATA SOURCES statements for specific systems.

The DEFAULT DATA SOURCES Statement has the following format:

DEFAULT DATA SOURCES - datasource1 datasource2 datasourcen

where datasourcen is a value taken from the list under DATA SOURCES.

### 7.3.1.8 IBMTCP SMF and DEFAULT IBMTCP SMF Statements

#### IBMTCP SMF

-----

This statement is required only when you have coded TCP on the DATA SOURCE statement, and you must override the default TCP SMF record type that is defined with DEFAULT IBMTCP SMF.

The purpose of this statement is to define the SMF record type, 118 or 119, so that the z/OS Communication Server is configured for generation. Each statement uniquely identifies the SMF record type from a specific system that will be processed and saved in the CA MICS database. You can specify a unique SMF record type for an ORGSYSID that will allow you to process SMF record type 118 for one ORGSYSID while processing SMF record type 119 for another.

This statement must follow the DATA SOURCE statement and precede another NETWORK ID or ORGSYSID statement. An error message is issued if the statement is not coded in the proper order.

The IBMTCP SMF statement has the following format:

IBMTCP SMF = nnn

where nnn is SMF record type 118 or 119.

#### DEFAULT IBMTCP SMF

-----

Use this optional statement to specify a default SMF record type for data produced by the z/OS Communication Server for TCP/IP network. TCP/IP can be configured to generate SMF record type 118, SMF record type 119, or both simultaneously.

The following rules apply regarding this statement:

- o This keyword must be coded after the first NETWORK ID statement and before the first ORGSYSID statement.
- o If this keyword is coded, the specified SMF record type (nnn) will be used as the IBMTCP SMF record type for each DATA SOURCES statement that includes TCP, UNLESS overridden with an IBMTCP SMF nnn statement that follows the DATA SOURCES statement.

The DEFAULT IBMTCP SMF statement has the following format:

DEFAULT IBMTCP SMF = nnn

where nnn is SMF record type 118 or 119.

Notes:

The SMF record type must either be 118 or 119, and, if coded, you must ensure that the same SMF record types are present on the INPUTSOURCE statement in sharedprefix.MICS.GENLIB(SNTGENIN).

If you update the SNTGENIN, do the following:

1. Submit sharedprefix.MICS.CNTL(SNTCGEN).
2. Edit prefix.MICS.PARMS(JCLGENU) so that it contains no values. If values are present, remove them.
3. Submit prefix.MICS.CNTL(JCLGENU).
4. Submit prefix.MICS.CNTL(SNTPGEN).

### 7.3.1.9 NETSPY SMF and DEFAULT NETSPY SMF Statements

#### NETSPY SMF

-----

The purpose of this statement is to define the SMF record type that CA NetSpy generates. You can use it to override the default NETSPY SMF record type that is defined with DEFAULT NETSPY SMF. You can also use it to define the SMF record type when there is no DEFAULT NETSPY SMF statement.

You can specify multiple statements (only one per ORGSYSID group) if you have more than one CA NetSpy product running on different systems, each generating SMF records that you want to process with the CA MICS Network Analyzer product. Each statement uniquely identifies the SMF record number from a specific system that will be processed and saved in the CA MICS database.

This statement must follow the DATA SOURCE statement and precede another NETWORK ID or ORGSYSID statement. An error message is issued if the statement is not coded in the proper order.

The NETSPY SMF statement has the following format:

NETSPY SMF = nnn

where nnn is a valid SMF record type in the range of 128 to 255 and cannot be blank.

#### DEFAULT NETSPY SMF

-----

Use this optional statement to specify a default SMF record type for data produced by CA NetSpy. Omit this statement if your data center does not use CA NetSpy or you do not want to process CA NetSpy data in the unit.

The following rules apply regarding this statement:

- o This keyword must be coded after the first NETWORK ID statement and before the first ORGSYSID statement.
- o If this keyword is coded, the specified SMF record type (nnn) will be used as the NETSPY SMF record type for each DATA SOURCES statement that includes NSPY, UNLESS overridden with a NETSPY SMF nnn statement that follows the DATA SOURCES statement.



The DEFAULT NETSPY SMF statement has the following format:

```
DEFAULT NETSPY SMF = nnn
```

where nnn is a valid SMF record type in the range of 128 to 255 and cannot be blank.

Notes:

If you specify SMF record types using either of these statements in `prefix.MICS.PARMS(SNTOPS)`, you must ensure that the same SMF record types are present on the `INPUTSOURCE` statement in `sharedprefix.MICS.GENLIB(SNTGENIN)`.

If you update the `SNTGENIN`, do the following:

1. Submit `sharedprefix.MICS.CNTL(SNTCGEN)`.
2. Edit `prefix.MICS.PARMS(JCLGENU)` so that it contains no values. If values are present, remove them.
3. Submit `prefix.MICS.CNTL(JCLGENU)`.
4. Submit `prefix.MICS.CNTL(SNTPGEN)`.

### 7.3.1.10 NETTCP SMF and DEFAULT NETTCP SMF Statements

#### NETTCP SMF

-----

This statement is required only when you have coded NTCP on the DATA SOURCE statement, you must override the default record type for CA NetMaster for TCP/IP that is defined with DEFAULT NETTCP SMF. The purpose of this statement is to define the SMF record type that your CA NetMaster for TCP/IP product generates. Each statement uniquely identifies the SMF record number from a specific system that will be processed and saved in a CA MICS database.

You can specify multiple statements (only one per ORGSYSID group) if you have more than one CA NetMaster for TCP/IP product running on different systems, each generating SMF records that you want to process with CA MICS Network Analyzer.

This statement must follow the DATA SOURCE statement and precede another NETWORK ID or ORGSYSID statement. An error message is issued if the statement is not coded in the proper order.

The NETTCP SMF statement has the following format:

NETTCP SMF = nnn

where nnn is a valid SMF record type in the range of 128 - 255 and cannot be blank.

#### DEFAULT NETTCP SMF

-----

Use this optional statement to specify a default SMF record type for data produced by CA NetMaster for TCP/IP. Omit this statement if your data center does not use NetTCP or if you do not want to process NetTCP data in the unit.

The following rules apply regarding this statement:

- o This keyword must be coded after the first NETWORK ID statement and before the first ORGSYSID statement.
- o If this keyword is coded, the specified SMF record type (nnn) will be used as the NETTCP SMF record type for each DATA SOURCES statement that includes NTCP, UNLESS overridden with a NETTCP SMF nnn statement that follows the DATA SOURCES statement.

The DEFAULT NETTCP SMF statement has the following format:

```
DEFAULT NETTCP SMF = nnn
```

where nnn is a valid SMF record type in the range of 128 to 255 and cannot be blank.

**Notes:**

If you specify SMF record types using either statement in `prefix.MICS.PARMS(SNTOPS)`, you must ensure that the same SMF record types are present on the `INPUTSOURCE` statement in `sharedprefix.MICS.GENLIB(SNTGENIN)`.

If you update the `SNTGENIN`, do the following:

1. Submit `sharedprefix.MICS.CNTL(SNTCGEN)`.
2. Edit `prefix.MICS.PARMS(JCLGENU)` so that it contains no values. If values are present, remove them.
3. Submit `prefix.MICS.CNTL(JCLGENU)`.
4. Submit `prefix.MICS.CNTL(SNTPGEN)`.

### 7.3.1.11 DELETEMS and DEFAULT DELETEMS Statements

#### DELETEMS

-----

This statement is optional and appropriate ONLY for data produced by CA NetSpy. This statement only applies if BOTH of the following conditions are true:

- o You want the Analyzer to process data from the CA NetSpy VTAM interface.
- o Data is collected in conjunction with a multiple session manager application that supports the CA NetSpy multiple session manager interface.

The DELETEMS statement has the following format:

DELETEMS nnn

where: nnn is either YES or NO. Specifying DELETEMS YES causes CA MICS Network Analyzer to delete observations in the SNTNSS file for sessions between the terminal and the multiple session manager applications used by the site, thus eliminating potentially redundant data.

You must include a separate DELETEMS YES statement for each CA NetSpy host (identified by NETWRKID and ORGSYSID) on which a multiple session manager application resides.

#### DEFAULT DELETEMS

-----

This optional statement is used to specify a default value for DELETEMS. The value defined with this keyword applies to every NSPY implicit/explicit DATA SOURCES option defined within the network, although it can be overridden by explicitly coding DELETEMS YES or DELETEMS NO for a specific system.

The DEFAULT DELETEMS statement has the following format:

DEFAULT DELETEMS nnn

where: nnn is either YES or NO. Specifying DEFAULT DELETEMS YES causes CA MICS Network Analyzer to delete observations in the SNTNSS file for sessions between the terminal and the multiple session manager application used by the site, thus

eliminating potentially redundant data.

GENERAL NOTES FOR THESE STATEMENTS

-----

Chapter 6 describes these data redundancy considerations, the operation of this Network Analyzer feature, and important issues you should be aware of when invoking this feature. Review Chapter 6 carefully since use of this feature may result in eliminating data that is meaningful to you for network analysis.

### 7.3.1.12 WORK, MULTWORK, and NOMULT Statements

WORK  
----

This statement is optional. It enables sites experiencing either SAS WORK space allocation problems or out of work space conditions during DAYnnn or INCRnnn (where nnn is the job step number), daily or incremental update processing, to allocate multiple WORK files.

You can allocate multiple WORK files for use during the daily and/or incremental update job step. The maximum number of WORK files you can allocate varies by product. These additional work files are used in conjunction with the single work data set allocated by default using the JCLDEF parameters WORKUNIT and WORKSPACE.

Because the individual space allocation requirement for each WORK file is typically much smaller, it is more likely to be satisfied.

To take advantage of multiple WORK files support, edit prefix.MICS.PARMS(cccOPS) and insert a WORK statement as shown below:

```
WORK n data_set_allocation_parameters
```

where n is the number of WORK data sets

NOTE: The default is zero (0).  
The maximum is nine (9).

data\_set\_allocation\_parameters is one or more data set allocation parameters (for example, STORCLAS or SPACE) separated by spaces.

You can also specify the WORK parameter as the following:

```
WORK n XXX pppp ssss
```

where:

n is the number of WORK data sets  
XXX is TRK or CYL  
pppp is the primary allocation  
ssss is the secondary allocation

Note: When allocating any number of SAS WORK data sets, be aware that one additional SAS WORK data set is automatically allocated to facilitate sorting. For example, if you allocate six SAS WORK data sets, you will actually get seven.

If you omit the `data_set_allocation_parameters` or the `WORK` parameter, the work data sets are allocated according to the values you specified for the `WORKUNIT` and `WORKSPACE` parameters in `prefix.MICS.PARMS(JCLDEF)`. Use the `data_set_allocation_parameters` to override this default, either to alter the space allocation or to use System Managed Storage (SMS) parameters to control data set placement and characteristics.

Note: If you allocate insufficient space for the WORK data sets, `DAYnnn` and/or `INCRnnn` processing will fail and can only be restarted from the beginning.

Note: If internal step restart is active, you can override the WORK data set allocation parameters at execution-time using the `//PARMOVRD` facility. For more information about execution-time override of dynamic data set allocation parameters, see the PIOM, section 2.3.6.

Specify data set allocation parameters, separated by blanks, according to SAS LIBNAME statement syntax. If you need multiple lines, repeat the `WORK` keyword on the continuation line.

WORK accepts the engine/host options documented in the SAS Companion for the z/OS environment, including `STORCLAS`, `UNIT`, `SPACE`, `BLKSIZE`, `DATACLAS`, `MGMTCLAS`, and `VOLSER`.

Important! Do not specify the `DISP` parameter.

Example 1:

```
WORK n STORCLAS=MICSTEMP SPACE=(XXX,(pppp,ssss),RLSE)
```

where:

- `n` - is the number of WORK data sets.
- `STORCLAS` - specifies a storage class for a new data set.  
The name can have up to 8 characters.
- `SPACE` - specifies how much disk space to provide for a new data set being allocated.
- `XXX` - is TRK or CYL.
- `pppp` - is the primary allocation.

ssss - is the secondary allocation.  
RLSE - specifies that free-space should be released  
when the data set is closed.

Example 2:

```
WORK n XXX pppp ssss
```

where:

n - is the number of WORK data sets.  
XXX - is TRK or CYL.  
pppp - is the primary allocation.  
ssss - is the secondary allocation.

Example 3 (multiple lines):

```
WORK n STORCLAS=MICSTEMP UNIT=SYSDA
WORK SPACE=(xxxx,(pppp,ssss),,,ROUND))
```

where:

n - is the number of WORK data sets.  
STORCLAS - specifies a storage class for a new data set.  
The name can have up to eight characters.  
UNIT - specifies the generic unit for a new data set.  
The name can have up to eight characters.  
SPACE - specifies how much disk space to provide for  
a new data set being allocated.  
XXX - is TRK or CYL.  
pppp - is the primary allocation.  
ssss - is the secondary allocation.

Note: Since there is some performance impact when using multiple WORK files, you should specify the minimum number of WORK data sets to meet your work space requirements. As a start, try incrementing the number gradually beginning from the default.

WORK Considerations

-----

How Much Space Should You Allocate?

o First Time Implementation of Multiple Work Files

If this is the first time you are implementing multiple work files for this product in this unit, review



prefix.MICS.PARMS(JCLDEF) and find the WORKSPACE parameter. It will resemble this sample statement:

```
WORKSPACE TRK 500 250
```

The value shows the current SAS WORK space allocation for the unit as a single data set. It also serves as the default value used in the unit's DAYnnn daily update (and/or INCRnnn incremental update) step unless you provide a WORK parameter.

To achieve the equivalent work space allocation of WORKSPACE TRK 500 250 using multiple WORK data sets that will collectively share the work space requirements of the daily and/or incremental update step, you could code either one of these:

```
WORK 2 SPACE=(TRK,(250,125))
```

```
WORK 5 SPACE=(TRK,(100,50))
```

To determine the total work space, multiply the number of WORK files (n) by the primary (pppp) and secondary (ssss) values specified.

Note: To simplify the example, only the SPACE parameter is shown above. You can follow either with data set allocation parameters like UNIT or STORCLAS as required for your site.

o Adjusting Allocation for Existing Multiple WORK Files

If you have previously implemented multiple WORK file support for this product in this unit, and you want to change either the number of WORK files or the space allocations, examine prefix.MICS.PARMS(cccOPS) and find the existing WORK statement.

- If the existing WORK statement only specifies the number of WORK files but does not contain space allocation information as shown below:

```
WORK 5
```

Then each of the multiple WORK files is allocated using the values from the WORKSPACE parameter of prefix.MICS.PARMS(JCLDEF), as described earlier under First Time Implementation of Multiple Work Files.

To increase workspace, you can increase the number of WORK files (for example, change WORK 5 to WORK 6,7,8, or 9), increase the space allocation in the WORKSPACE parameter, or do both.

To decrease workspace, you can decrease the number of WORK files (for example, change WORK 5 to WORK 4,3,2, or 1), decrease the space allocation in the WORKSPACE parameter, or do both.

You can also elect to explicitly specify the multiple WORK file space allocation by adding the space allocation values directly to the WORK statement. This will remove the link to the prefix.MICS.PARMS(JCLDEF) WORKSPACE parameter for multiple WORK file space allocation. This is recommended as it serves to clearly document, in one place, how multiple WORK files are allocated.

- If the existing WORK statement does include space allocation as shown in the examples below:

```
WORK 5 TRK 200 100
```

or

```
WORK 5 SPACE=(TRK,(200,100)) STORCLAS=MICSTEMP
```

Simply change the values to meet your needs.

If you need more work space, you can increase the number of WORK files (for example, change WORK 5 to WORK 6,7,8, or 9), increase the space allocation (for example, change TRK 200 100 to TRK 250 120), or do both.

To decrease work space, you can decrease the number of WORK files (for example, change WORK 5 to WORK 4,3,2, or 1), decrease the space allocation (for example, change TRK 200 100 to TRK 150 80), or do both.

Note: If internal step restart is NOT active (RESTART NO) and you change the WORK parameter, you must:

- o Run cccPGEN
- o Run JCLGENU for DAILY (to regenerate DAILY) and, if incremental update is enabled, INCRccc

When internal step restart is active, (RESTART YES), then,

when you change WORK and run cccPGEN, changes take effect immediately. There is no need to run JCLGENU.

SASWORK  
-----

This statement is optional.

The WORK DD statement in the CA MICS procedures allocates a temporary data set where SAS keeps its temporary data files and other items that SAS uses during processing of the current job.

By default, the space allocated is defined in the member prefix.MICS.PARMS(JCLDEF) with the WORKSPACE and WORKUNIT parameters, then generated into all the JCL procedures for a given unit.

With the SASWORK statement you have the option to override this unit-wide definition to specify the space allocation individually for the current step.

The format of the SASWORK statement is:

SASWORK data\_set\_allocation\_parameters

where data\_set\_allocation\_parameters is one or more data set allocation parameters (for example, STORCLAS or SPACE) separated by spaces.

You can also specify the SASWORK parameter as the following:

SASWORK XXX pppp ssss

where:

XXX is TRK or CYL  
pppp is the primary allocation  
ssss is the secondary allocation

If you omit the data\_set\_allocation\_parameters or the SASWORK statement, the WORK data set is allocated according to the values you specified for the WORKUNIT and WORKSPACE parameters in prefix.MICS.PARMS(JCLDEF). Use the data\_set\_allocation\_parameters to override this default, either to alter the space allocation or to use System Managed Storage (SMS) parameters to control data set placement and characteristics.

Specify data set allocation parameters, separated by blanks, according to SAS LIBNAME statement syntax. If you need multiple lines, repeat the SASWORK keyword on the continuation line.

Example:

```
SASWORK STORCLAS=MICSTEMP SPACE=(XXX,(pppp,ssss))
```

where:

|          |                                                                                          |
|----------|------------------------------------------------------------------------------------------|
| STORCLAS | - specifies a storage class for a new data set.<br>The name can have up to 8 characters. |
| SPACE    | - specifies how much disk space to provide for<br>a new data set being allocated.        |
| XXX      | - is TRK or CYL.                                                                         |
| pppp     | - is the primary allocation.                                                             |
| ssss     | - is the secondary allocation.                                                           |

Note: If you change the SASWORK parameter, you must:

- o Run cccPGEN
- o Run JCLGENU for DAILY (to regenerate DAILY) and, if incremental update is enabled, INCRccc

```
MULTWORK|NOMULT fff fff ... fff
```

```

```

Since multiple work files usage impacts performance, this product provides these optional parameters so you can restrict multiple work files usage to only those files having excessive space requirements.

Note: You can only use one of these optional parameters with the WORK statement, NOT both.

The MULTWORK parameter restricts the use of multiple WORK files to ONLY those listed after the MULTWORK keyword.

```
MULTWORK fff fff ... fff
```

where fff is the unique three character identifier

If you need multiple lines, repeat the MULTWORK on the continuation line.

The NOMULT parameter forces the use of multiple WORK files for all files EXCEPT those specified after the NOMULT keyword.

```
NOMULT fff fff ... fff
```

where fff is the unique three character identifier

If you need multiple lines, repeat the NOMULT on the continuation line.

The default is

```
MULTWORK PSW NNW NIN NCL NAF GAF LNF NSF NEF NLW NVR NSS
MULTWORK NSP NAC NOD NSC RTE NSV VBF RTM NSA LGN LGF STN
MULTWORK CTN FSF FCF API INI TRM NLP LGM LGE INH TRL NAT
MULTWORK NTW NPT NST NTS TCS APJ FCG FSG CTM STM
```

if neither MULTWORK or NOMULT parameters are specified.

The following files are eligible for multiple WORK support:

#### SNT Network Information Area Files

|       |                                                                      |
|-------|----------------------------------------------------------------------|
| NAC   | NCP Network Accounting File                                          |
| NCL   | NCP Link File                                                        |
| NAF   | NCP Activity File                                                    |
| NIN   | Network Incident File                                                |
| NNW   | Network Comp Activity Work File (Internal work file Parallel to CAF) |
| NSV   | NLDM Service File                                                    |
| LNF   | LAN File                                                             |
| GAF   | Generic Alert File                                                   |
| NEF   | NPDA Event File                                                      |
| NSF   | NPDA Statistical File                                                |
| NSP   | CA NetSpy Application (PLU) Activity File                            |
| NSS   | CA NetSpy Terminal (SLU) Activity File                               |
| NLP   | NCP Line Processor Activity File                                     |
| NTS   | CA NetSpy TCP/IP Telnet Server File                                  |
| TCS   | CA NetSpy TCP/IP Stack Entry File                                    |
| PSW   | NPM User Activity File (Internal work file Parallel to PSU)          |
| NVR   | CA NetSpy Virtual Route Activity File                                |
| * NAT | NCP Network Accounting File (Internal work file Parallel to NAC)     |
| * NPT | CA NetSpy Application (PLU) Activity File (Internal                  |

work File Parallel to NSP)  
\* NST CA NetSpy Terminal (SLU) Activity File (Internal  
work file Parallel to NSS)

#### NVS Netview Session Information Area Files

NLL NLDM Link Activity File  
NLW An internal work file used in conjunction with the NOD  
file during SNT daily processing, to create files in  
the NVS information area, including LSY (NLDM System  
PLU Activity File) and NLL (NLDM Link Activity File)  
\*NTW An internal work file used in conjunction with the NLW  
file during SNT daily processing, to create files in  
the NVS information area  
NOD An internal work file used in conjunction with the NLW  
file during SNT daily processing, to create files in  
the NVS information area  
NSA NLDM Session Accounting File  
NSC NLDM Session Connectivity File  
RTE NLDM Route File  
RTM NLDM Response Time File  
VBF NLDM VTAM Bind Failure File

#### TCP Transport Communication Protocol/Internet Protocol

STN Telnet Server File  
CTN Telnet Client File  
FSF FTP Server File  
FCF FTP Client File  
API API Calls for Sockets File  
STM Telnet Server File (SMF 119)  
CTM Telnet Client File (SMF 119)  
FSG FTP Server File (SMF 119)  
FCG FTP Client File (SMF 119)  
APJ API Calls for Sockets File (SMF 119)  
LGN Telnet Server Logon Records File  
LGF Telnet Server Logoff Records File  
\*LGM Telnet Server Logon Records File  
\*LGE Telnet Server Logoff Records File  
INI API Calls for Sockets INIT Records File  
TRM API Calls for Sockets TERM Records File  
\*INH API Calls for Sockets INIT Records File  
\*TRL API Calls for Sockets TERM Records File

The following section discusses changing the WORK option:

- 1 - Change the Number of Work Files

## New Topic

To change the number of work files used in the CA MICS Network Analyzer processing in Step DAY056, follow the checklist provided below for each unit.

```

* *
* CHANGE NUMBER OF WORK FILES *
* *

```

- \_\_\_ 1. Update the WORK statement in prefix.MICS.PARMS(cccOPS), where (ccc) is the component identifier, to specify the number of work data sets required. Below is an example:

```
WORK n STORCLAS=MICSTEMP SPACE=(XXX,(pppp,ssss))
```

where:

|          |                                                                                           |
|----------|-------------------------------------------------------------------------------------------|
| n        | - is the number of WORK data sets.                                                        |
| STORCLAS | - specifies a storage class for a new data set. The name can have up to eight characters. |
| SPACE    | - specifies how much disk space to provide for a new data set being allocated.            |
| XXX      | - is TRK or CYL.                                                                          |
| pppp     | - is the primary allocation.                                                              |
| ssss     | - is the secondary allocation.                                                            |

You should specify the minimum number of WORK data sets to meet your work space requirements. As a start, try incrementing the number gradually beginning from the default.

- \_\_\_ 2. If this is the first time you are implementing multiple work files for this product, then continue with Step 2. If you are just changing the number currently in use, or simply the space definitions, then proceed to Step 3 of this checklist.

Browse sharedprefix.MICS.PROTOLIB(DYcccnnn) and sharedprefix.MICS.PROTOLIB(cccINCR), where (nnn) is the job step number and (ccc) is the product ID for this product, checking for the presence of the WORK symbolic on the EXEC statement to determine if you have previously modified this product to increase the allocation of SAS WORK space.

- \_\_\_ 2a. If you find a WORK symbolic, simply divide the primary and secondary allocation values from the WORK symbolic by the number of work files specified above (value of n on the WORK statement coded in Step 1).

Coding the resulting values will yield the same aggregate space allocation you have been using with a single WORK file. To double your available WORK space, carry out the division, double the results and use the values in the WORK definition above.

- \_\_\_ 2b. If you did not find a WORK symbolic in PROTOLIB, examine prefix.MICS.PARMS(JCLDEF) for each CA MICS unit containing this product. Find the WORKSPACE keyword. The space allocation specified is used for a single SAS WORK file. Perform the same division as described in the previous paragraph to determine the quantity that will yield equivalent total allocation with multiple WORK files. Then adjust the values upward to meet your needs.

- \_\_\_ 3. Submit the job in prefix.MICS.CNTL(cccPGEN).

- \_\_\_ 4. If you specified RESTART YES in the product's cccOPS, you are done. Otherwise, you must do Steps 5, 6, and 7.

- \_\_\_ 5. Edit prefix.MICS.PARMS(JCLGENU) so that it contains a single line that reads:

DAILY

or, if incremental update is enabled for this product in this unit database, specify:

DAILY INCRccc

where ccc is the product ID.

- \_\_\_ 6. Submit the job in prefix.MICS.CNTL(JCLGENU). Ensure that there are no error messages in MICSLOG or SYSTSPRT, that the MICSLOG contains the normal termination message, BAS10999I, and that the job completes with a condition code of zero.

- \_\_\_ 7. The following operational job(s) have changed:

DAILY



INCRccc (if incremental update is enabled)

If your site has implemented the operational CA MICS processes in a scheduling product, the JCL may have to be refreshed in that product. See the scheduling product's administrator for the exact processes involved in updating that product's representation of the CA MICS jobs.

### 7.3.1.13 Internal Step Restart Statements

RESTART YES/NO

-----

This statement is optional. Specify this to activate internal step restart for this product's DAILY and/or INCRccc database update job steps:

RESTART YES

If you do not specify or enable the RESTART parameter, then this option defaults to the following and internal step restart is disabled:

RESTART NO

```

* *
* Note: Changing the RESTART parameter (either from NO *
* to YES or from YES to NO) requires regeneration *
* of the DAILY operational job by executing *
* prefix.MICS.CNTL(JCLGEN) or by specifying *
* DAILY in prefix.MICS.PARMS(JCLGEN) and *
* executing prefix.MICS.CNTL(JCLGEN). *
* *
* If incremental update is active for this product, *
* you must also regenerate the INCRccc job. *
* *

```

Internal step restart can significantly reduce time and resource usage to recover from daily and/or incremental update processing failures. CA MICS uses a checkpoint/restart technique.

- o When internal step restart is activated, the database update job step "checkpoints" (or saves) intermediate results (work file contents) and the operational environment at the end of each processing phase.
- o Then, if required, the database update step can resume execution at the beginning of the processing phase in which the failure occurred.
- o Restart is accomplished by restoring the operational

environment from the last checkpoint, bypassing completed processing phases, and resuming execution using intermediate results (work files) from the last checkpoint.

Note: When you activate internal step restart (RESTART YES), the following optional restart parameters are enabled. These parameters have no effect if restart is disabled (RESTART NO). For more details, see the individual parameter descriptions later in this section.

- o RESTARTCKPT data\_set\_allocation\_parameters
- o RESTARTWORK data\_set\_allocation\_parameters
- o DYNAMWAIT minutes

#### Processing Phases:

-----

This product employs two database update processing phases followed by the two common roll-up phases:

| Phase    | Description                                                                                                                                                                                                     |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -----    |                                                                                                                                                                                                                 |
| FORMAT   | Read raw input data, convert to SAS format, and output to intermediate work files.                                                                                                                              |
| DBUPDATE | Sort intermediate work file contents, eliminate duplicate input data, prepare for DETAIL cycle creation, merge data across optional multiple work files, enhance data content, and create the new DETAIL cycle. |
| DYSUM    | Summarize DETAIL data to create new DAYS cycles and to update current week-to-date and month-to-date cycles.                                                                                                    |
| DYAGE    | Cutover new database cycles to production and "age" existing cycles.                                                                                                                                            |

#### RESTART Considerations

-----

### o Overhead

Enabling internal step restart adds some overhead to the database update job step -- the cost of taking checkpoints and managing saved materials. Since this overhead is relatively constant and independent of input data volume, you may find that costs outweigh potential savings when input data volume is low, for example in a test unit. For high volume, production units, internal step restart support overhead should be a minor portion of total resource usage.

### o Cataloged Work Files

When internal step restart is enabled, the SAS work data set, internal step restart control data set, and multiple work file data sets are allocated and cataloged with permanent dataset names so they will be retained for use in restart if the step abends. These data sets are deleted when the step completes successfully.

Prior to enabling internal step restart support, these data sets were probably allocated on system "scratch" space with a temporary, system assigned data set names. If your installation standards do not allow "permanent" data sets on DASD volumes used for temporary work space, you may need to use the WORK, RESTARTCKPT, and RESTARTWORK parameters to direct the internal step restart data sets to a generic unit or storage class that allows cataloged data sets.

### o Dynamic Allocation

When internal step restart is active, dynamic allocation is employed for the work data sets. If your installation restricts dynamic allocation of large, cataloged data sets, you may need to use the WORK, RESTARTCKPT, and RESTARTWORK parameters to direct work data set allocation to a generic unit or storage class where dynamic allocation is allowed.

### o Data Set Names

The SAS work data set, internal step restart control data set, and multiple work file data sets are allocated and cataloged according to the standard CA MICS unit database data set name conventions. The default DDNAME and data set names are:

- o SAS work data set,  
    //cccXWORK DD DSN=prefix.MICS.cccXWORK,.....
- o Internal step restart control data set,  
    //cccXCKPT DD DSN=prefix.MICS.cccXCKPT,.....
- o Multiple work file data sets,  
    //WORKnn DD DSN=prefix.MICS.cccWRKnn,.....

Since these data sets conform to the same data set name conventions as your existing CA MICS data sets, there should be few, if any, data set name related allocation issues. However, it is possible to override the data set names if required. Please contact CA MICS Product Support for assistance if you must alter data set names.

#### RESTARTCKPT

-----

This statement is optional. Specify the following to override default data set allocation parameters for the internal step restart checkpoint data set:

RESTARTCKPT data\_set\_allocation\_parameters

Note: RESTARTCKPT is ignored when you specify RESTART NO.

The internal step restart checkpoint data set (or cccXCKPT data set) contains processing status, control, and SAS environmental information for internal step restart processing checkpoints. This includes a copy of the SAS WORK format and macro catalogs, current macro variable values, and a description of work files that may be needed to restart DAYnnn processing.

By default, the cccXCKPT data set is allocated according to the values you specified for the WORKUNIT and WORKSPACE parameters in prefix.MICS.PARMS(JCLDEF). Specify RESTARTCKPT to override this default, either to alter the space allocation or to use System Managed Storage (SMS) parameters to control data set placement and characteristics.

Note: If you allocate insufficient space for the cccXCKPT data set, DAYnnn processing will fail and can only be restarted from the beginning.

Note: You can override the RESTARTCKPT data set allocation

parameters at execution-time using the //PARMOVRD facility. For more information about execution-time override of dynamic data set allocation parameters, see the PIOM, section 2.3.6.

Specify data set allocation parameters, separated by blanks, according to SAS LIBNAME statement syntax. If you need multiple lines, repeat the RESTARTCKPT keyword on the continuation line.

RESTARTCKPT accepts the engine/host options documented in the SAS Companion for the z/OS Environment, including STORCLAS, UNIT, SPACE, BLKSIZE, DATACLAS, MGMTCLAS, and VOLSER.

Important! DO NOT SPECIFY THE DISP PARAMETER.

Example 1:

```
RESTARTCKPT STORCLAS=MICSTEMP SPACE=(xxxx,(pp,ss),,,ROUND)
```

where:

STORCLAS - specifies a storage class for a new data set.  
The name can have up to eight characters.

SPACE - specifies how much disk space to provide for a new data set being allocated, where:

xxxx is TRK, CYL, or blklen  
pp is the primary allocation  
ss is the secondary allocation

and ROUND specifies that the allocated space be "rounded" to a cylinder boundary when the unit specified was a block length. ROUND is ignored with the TRK or CYL options.

Example 2 (multiple lines):

```
RESTARTCKPT STORCLAS=MICSTEMP UNIT=SYSDA
RESTARTCKPT SPACE=(xxxx,(pp,ss),,,ROUND)
```

where:

STORCLAS - specifies a storage class for a new data set.  
The name can have up to eight characters.

UNIT - specifies the generic unit for a new data set.  
The name can have up to eight characters.

SPACE - specifies how much disk space to provide for a new data set being allocated.

#### RESTARTWORK

-----

This statement is optional. Specify the following to override default data set allocation parameters for the internal step restart WORK data set:

RESTARTWORK data\_set\_allocation\_parameters

Note: RESTARTWORK is ignored when you specify RESTART NO.

The internal step restart WORK data set (or cccXWORK data set) contains the intermediate work files that are not enabled to multiple work file support, including those files you may have specified on the optional NOMULT statement.

By default, the cccXWORK data set is allocated according to the values you specified for the WORKUNIT and WORKSPACE parameters in prefix.MICS.PARMS(JCLDEF). Specify RESTARTWORK to override this default, either to alter the space allocation or to use System Managed Storage (SMS) parameters to control data set placement and characteristics.

Note: If you allocate insufficient space for the cccXWORK data set, DAYnnn processing will fail and can only be restarted from the beginning.

Note: You can override the RESTARTWORK data set allocation parameters at execution-time using the //PARMOVRD facility. For more information about execution-time override of dynamic data set allocation parameters, see the PIOM, section 2.3.6.

Specify data set allocation parameters, separated by blanks, according to SAS LIBNAME statement syntax. If you need multiple lines, repeat the RESTARTWORK keyword on the continuation line.

RESTARTWORK accepts the engine/host options documented in "SAS Companion for the z/OS Environment", including STORCLAS, UNIT, SPACE, BLKSIZE, DATACLAS, MGMTCLAS, and VOLSER.

Important! DO NOT SPECIFY THE DISP PARAMETER.

Example 1:

```
RESTARTWORK STORCLAS=MICSTEMP SPACE=(xxxx,(pp,ss),,,ROUND)
```

where:

STORCLAS - specifies a storage class for a new data set.  
The name can have up to eight characters.

SPACE - specifies how much disk space to provide for  
a new data set being allocated, where:

xxxx is TRK, CYL, or blklen

pp is the primary allocation

ss is the secondary allocation

and ROUND specifies that the allocated space be  
"rounded" to a cylinder boundary when the unit  
specified was a block length. ROUND is ignored  
with the TRK or CYL options.

Example 2 (multiple lines):

```
RESTARTWORK STORCLAS=MICSTEMP UNIT=SYSDA
```

```
RESTARTWORK SPACE=(xxxx,(pp,ss),,,ROUND)
```

where:

STORCLAS - specifies a storage class for a new data set.  
The name can have up to eight characters.

UNIT - specifies the generic unit for a new data set.  
The name can have up to 8 characters.

SPACE - specifies how much disk space to provide for  
a new data set being allocated.

The following section discusses enabling this option:

- 1 - Enable Internal Step Restart



### 7.3.1.13.1 Enable Internal Step Restart

To enable the internal step restart in the CA MICS Network Analyzer, follow the checklist provided below for each unit:

```

* *
* ENABLE INTERNAL STEP RESTART *
* *

```

- \_\_\_ 1. Edit prefix.MICS.PARMS(cccOPS), where (ccc) is the component identifier, and specify:

RESTART YES

For additional information on related topic, review the documentation for this product on WORK, RESTARTWORK, and RESTARTCKPT parameters to override default data set allocation parameters.

- \_\_\_ 2. Submit the job in prefix.MICS.CNTL(cccPGEN).
- \_\_\_ 3. Edit prefix.MICS.PARMS(JCLGENU) so that it contains a single line that reads:

DAILY

or, if incremental update is enabled for this product in this unit database, specify:

DAILY INCRccc

where ccc is the product ID.

- \_\_\_ 4. Submit the job in prefix.MICS.CNTL(JCLGENU). Ensure that there are no error messages in MICSLOG or SYSTSPRT, that the MICSLOG contains the normal termination message, BAS10999I, and that the job completes with a condition code of zero.

- \_\_\_ 5. The following operational job(s) have changed:

DAILY

INCRccc (if incremental update is enabled)

If your site has implemented the operational CA MICS

processes in a scheduling product, the JCL may have to be refreshed in that product. See the scheduling product's administrator for the exact processes involved in updating that product's representation of the CA MICS jobs.

### 7.3.1.14 Incremental Update Statements

INCRUPDATE

-----

This statement is optional. Specify this to enable incremental update for this product:

INCRUPDATE YES

If you do not specify or enable the INCRUPDATE parameter, then this option defaults to this and incremental update is disabled:

INCRUPDATE NO

```

*
* Note: Changing the INCRUPDATE parameter (either from NO
* to YES or from YES to NO) requires regeneration
* of the DAILY operational job by executing
* prefix.MICS.CNTL(JCLGEN) or by specifying
* DAILY in prefix.MICS.PARMS(JCLGEN) and
* executing prefix.MICS.CNTL(JCLGEN).
*
* If you specify INCRUPDATE YES, you must also
* generate the INCRccc, cccIUALC, and cccIUGDG jobs
* (where ccc is the 3 character product ID).
* Depending on the options you select, you may also
* need to execute the cccIUALC and/or cccIUGDG
* jobs.
*

```

Incremental update can significantly reduce time and resource usage in the DAILY job by letting you split out a major portion of daily database update processing into multiple, smaller, incremental updates executed throughout the day.

- o Standard CA MICS database update processing involves (1) reading and processing raw input data to generate DETAIL and DAYS level CA MICS database files, followed by (2) summarization of DETAIL/DAYS level data to update week-to-date and month-to-date database files.
- o When you activate incremental update:
  - You can execute the first-stage processing (raw data input to create DETAIL/DAYS files) multiple times

throughout the day, each time processing a subset of the total day's input data.

- Then, during the final update of the day (in the DAILY job), the incremental DETAIL/DAYS files are "rolled-up" to the database DETAIL and DAYS timespans, and then summarized to update the week-to-date and month-to-date files.
- o Incremental update is independent of your internal step restart or DBSPLIT specifications. You have the option to perform incremental updates with or without internal step restart support.
- o Incremental update is activated and operates independently by product. The incremental update job for this product, INCRccc (where ccc is the product ID), can execute concurrently with the incremental update job for another product in the same unit database.
- o The CA MICS database remains available for reporting and analysis during INCRccc job execution.

```

* *
* Note: CA MICS is a highly configurable system *
* supporting up to 36 unit databases, each of which *
* can be configured and updated independently. *
* Incremental update is just one of the options you *
* can use to configure your CA MICS complex. *
* *
* All efforts should be made to employ CA MICS *
* configuration capabilities to minimize issues *
* prior to activating incremental update. For *
* example: *
* *
* o Splitting work to multiple units is an *
* effective way to enable parallel database *
* update processing *
* *
* o Adjusting account code definitions to ensure *
* adequate data granularity while minimizing *
* total database space and processing time *
* *
* o Tailoring the database to drop measurements *
* and metrics of lesser value to your *
* data center, thereby reducing database update *
* processing and resource consumption *
* *
```

```

* While incremental update is intended to reduce *
* DAILY job elapsed time, total resource usage of *
* the combined INCRccc and DAILY jobs steps can *
* increase due to the additional processing *
* required to maintain the incremental update *
* "to-date" files and for roll-up to the unit *
* database. The increased total resource usage *
* will be more noticeable with small data volumes, *
* where processing code compile time is a greater *
* percentage of total processing cost. *
* *

```

Note: When you activate incremental update (INCRUPDATE YES), the following optional incremental update parameters are enabled. These parameters have no effect if incremental update is disabled (INCRUPDATE NO). For more details, see the individual parameter descriptions later in this section.

- o INCRDB      PERM/TAPE/DYNAM
- o INCRDETAIL data\_set\_allocation\_parameters
- o INCRDAYS    data\_set\_allocation\_parameters
- o INCRCKPT    data\_set\_allocation\_parameters
- o INCRSPLIT   USE/IGNORE data\_set\_allocation\_parameters

Incremental update processing reads and processes raw measurement data to create and maintain DETAIL and DAYS level "to-date" files for the current day.

- o These incremental update database files are maintained on unique z/OS data sets, independent of the standard CA MICS database files, and independent of any other product's incremental update database files. There is one data set each for DETAIL and DAYS level "to-date" data and a single incremental update checkpoint data set for this product in this unit.
- o The incremental update DETAIL and DAYS files can be permanent DASD data sets, or they can be allocated dynamically as needed and deleted after DAILY job processing completes. Optionally, you can keep the incremental update DETAIL and DAYS files on tape, with the data being loaded onto temporary DASD space as needed for incremental update or DAILY job processing. See the INCRDB PERM/TAPE/DYNAM option for more

information.

After activating incremental update, you will use three incremental update facility jobs found in prefix.MICS.CNTL (Note that ccc is the product ID):

- o cccIUALC

You execute this job to allocate and initialize the incremental update checkpoint file, and optionally the incremental update DETAIL and DAYS database files. cccIUALC is generally executed just ONE time.

- o cccIUGDG

You execute this job to add generation data group (GDG) index definitions to your system catalog in support of the INCRDB TAPE option. cccIUGDG is generally executed just ONE time.

- o INCRccc

This is the job you execute for each incremental update. You will integrate this job into your database update procedures for execution one or more times per day to process portions of the total day's measurement data.

Note: The DAILY job is run once at the end of the day. It will perform the final incremental update for the day's data, and then roll-up the incremental DETAIL/DAYS files to the database DETAIL and DAYS timespans and update the week-to-date and month-to-date files.

#### INCRUPDATE Considerations

-----

- o Overhead

Incremental update is intended to reduce DAILY job resource consumption and elapsed time by offloading a major portion of database update processing to one or more executions of the INCRccc job. In meeting this objective, incremental update adds processing in the INCRccc and DAILY jobs to accumulate data from each incremental update execution into the composite "to-date" DETAIL and DAYS incremental update files, and also adds processing in the DAILY job to copy the incremental update files to the unit database DETAIL and DAYS

timespans. The amount of this overhead and the savings in the DAILY job are site-dependent, and will vary based on input data volume and on the number of times INCRccc is executed each day.

In addition, activating incremental update will cause additional compile-based CPU time to be consumed in the DAYnnn DAILY job step. The increase in compile time is due to additional code included for each file structure in support of the feature. This increase should be static based on the scope of the CA MICS data integration product in terms of files. This compile-time increase does not imply an increase in elapsed or execution time. Incremental update allows I/O bound, intensive processing (raw data inputting, initial CA MICS transformation, etc.) to be distributed outside of the DAILY job. I/O processing is the largest contributor to elapsed time in large volume applications. Thus, the expected overall impact is a decrease in the actual runtime of the DAYnnn job step.

- o Increased "Prime Time" Workload

By offloading work from the DAILY job to one or more INCRccc executions throughout the day, you are potentially moving system workload and DASD work space usage from the "off-hours," (when the DAILY job is normally executed) to periods of the day where your system resources are in highest demand. You should schedule INCRccc executions carefully to avoid adverse impact to batch or online workloads. For example, if your site's "prime shift" is 8:00 AM to 5:00 PM, you might choose to schedule incremental updates for 7:00 AM (just before "prime shift") and 6:00 PM (just after "prime shift"), with the DAILY job executing just after midnight.

- o Increased DASD Usage

The DASD space required for the incremental update DETAIL and DAYS database files is in addition to the DASD space already reserved for the CA MICS database. By default, the incremental update database files are permanently allocated, making this DASD space unavailable for other applications. In general, you can assume that the incremental update database files will require space equivalent to two cycles of this product's DETAIL and DAYS timespan files.

Alternatively, the incremental update database files can

be allocated in the first incremental update of the day and deleted by the DAILY job (see the INCRDB DYNAM option later in this section). This approach reduces the amount of time that the DASD space is dedicated to incremental update, and lets the amount of DASD space consumed increase through the day as you execute each incremental update.

A third option is to store the incremental update database files on tape (see the INCRDB TAPE option). With this approach, the DASD space is required just for the time that each incremental update or DAILY job step is executing. Note that while this alternative reduces the "permanent" DASD space requirement, the total amount of DASD space required while the incremental update or DAILY jobs are executing is unchanged. In addition, the TAPE option adds processing to copy the incremental update files to tape, and to reload the files from tape to disk.

Note: The incremental update checkpoint file is always a permanently allocated disk data set. This is a small data set and should not be an issue.

- o Operational Complexity

Incremental update expands your measurement data management and job scheduling issues. You must ensure that each incremental update and the DAILY job processes your measurement data chronologically; that is, each job must see data that is newer than the data processed by the prior job. By incrementally updating the database, you have more opportunities to miss a log file, or to process a log out of order.

- o Interval End Effects

Each incremental update processes a subset of the day's measurement data, taking advantage of early availability of some of the day's data, for example, when a measurement log fills and switches to a new volume. This can cause a problem if the measurement log split occurs while the data source is logging records for the end of a measurement interval, thus splitting the data for a single measurement interval across two log files. When an incremental update processes the first log file, the checkpoint high end timestamp is set to indicate that this split measurement interval has been processed. Then, when the rest of the measurement interval's data is



encountered in a later update, it can be dropped as duplicate data (because data for this measurement interval end timestamp has already been processed).

Appropriate scheduling of log dumps and incremental updates can avoid this problem. For example, if you plan to run incremental updates at 7:00 AM and 6:00 PM, you could force a log dump in the middle of the measurement interval just prior to the scheduled incremental update executions. This is an extension of the procedure you may already be using for end-of-day measurement log processing. The objective is to ensure that all records for each monitor interval are processed in the same incremental update.

- o Dynamic Allocation

When you activate incremental update and specify TAPE or DYNAM for the INCRDB parameter, dynamic allocation is employed for the incremental update database files. If your site restricts dynamic allocation of large, cataloged data sets, you must use the INCRDETAIL and INCRDAYS parameters to direct incremental update data set allocation to a generic unit or storage class where dynamic allocation is allowed.

- o Data Set Names

The incremental update database files are allocated and cataloged according to standard CA MICS unit database data set name conventions. The DDNAME and default data set names are (where ccc is the product ID):

- o Incremental update checkpoint file,  
//IUCKPT DD DSN=prefix.MICS.ccc.IUCKPT,.....
- o Incremental update DETAIL  
//IUDETAIL DD DSN=prefix.MICS.ccc.IUDETAIL,.....
- o Incremental update DAYS  
//IUDAYS DD DSN=prefix.MICS.ccc.IUDAYS,....

Since these data sets conform to the same data set name conventions as your existing CA MICS data sets, there should be few, if any, data-set-name-related allocation issues. However, it is possible to override the data set names if required. Contact Technical Support at <http://ca.com/support> for assistance if you must change data set names.

### INCRDB

-----

This statement is optional. The default is this:

INCRDB PERM

Note: INCRDB is ignored when you specify INCRUPDATE NO.

Specify this statement or take the default, to keep the incremental update database DETAIL and DAYS files on permanently allocated DASD data sets:

INCRDB PERM

Execute the prefix.MICS.CNTL(cccIUALC) job to allocate the incremental update database files.

```

*
* Note: The incremental update checkpoint file is always *
* a permanently allocated DASD data set. *
*

```

Specify this to offload the incremental update DETAIL and DAYS files to tape between incremental update executions:

INCRDB TAPE #gdgs UNIT=name

With the TAPE option, the incremental update DETAIL and DAYS DASD data sets are dynamically allocated at the beginning of the incremental update job or DAILY job step, and then are deleted after the job step completes.

- o The first incremental update job of the day allocates and initializes the incremental update database files. At the end of the job, the DETAIL and DAYS files are copied to a new (+1) generation of the incremental update tape data sets. Then the DASD files are deleted.
- o Subsequent incremental update jobs restore the DASD incremental update database files from the current, (0) generation, incremental update tape data sets before processing the input measurement data. At the end of

the job, the DETAIL and DAYS files are copied to a new (+1) generation of the incremental update tape data sets. Then the DASD files are deleted.

- o The DAILY job step also restores the DASD incremental update database files from the (0) generation tape files before processing the input data, but does NOT copy the incremental update database files to tape. Thus, the DAILY job actually creates a new, null (+1) generation.
- o Use the #gdgs parameter to specify the maximum number of incremental update tape generations. The minimum is 2 and the maximum is 99, with a default of 5.  
Set the number of generations equal to or greater than the number of incremental updates, including the DAILY job you plan to execute each day. This facilitates restart and recovery if you encounter problems requiring you to reprocess portions of the daily measurement data.
- o Use the optional UNIT=name parameter to specify a tape unit name for the incremental update database output tapes. The default is to use the same tape unit as the input tapes.
- o A special index must be created in your system catalog for each of the incremental update tape data set generation data groups. The prefix.MICS.CNTL(cccIUGDG) job will generate the statements to create the incremental update GDG index definitions.
  - Before each index is built, it is deleted. These DLTX (or DELETE) statements causes an error message if no entry exists. This is done so that you can change the number of entries without having to delete each of the index entries.
  - DLTX and BLDG (or DELETE and DEFINE) fail if there is a cataloged data set with the same index. IDCAMS (or IEHPROGM) issues a message and gives a return code of 8. This issue is not a problem for non-GDG entries or if the GDG already has the desired number of entries.
  - If you want to change the number of entries kept in a GDG with cataloged data sets, do the following:
    1. Uncatalog any existing entries in the GDG.
    2. Delete the index with a DLTX (or DELETE).

3. Create the index with a BLDG (or DEFINE).
  4. Catalog any entries that are uncataloged in step 1.
- o The incremental update tape data set names are as follows, where ccc is the product ID:
    - Incremental update tape DETAIL file  
tapeprefix.MICS.ccc.IUXTAPE.GnnnnV00
    - Incremental update tape DAYS file  
tapeprefix.MICS.ccc.IUDTAPE.GnnnnV00

```

*
* Note: The INCRDETAIL and INCRDAYS parameters are
* required when you specify INCRDB TAPE.
*

```

Specify this parameter to allocate dynamically the incremental update DETAIL and DAYS DASD data sets in the first incremental update of the day, and then delete these data sets at the end of the DAILY job step:

INCRDB DYNAM

- o With this option, no space is used for the incremental update database files during the time between the end of the DAILY job step and the beginning of the next day's first incremental update.
- o With this approach, you can set the data set allocation parameters so that the incremental update DETAIL and DAYS data sets start out with a minimum allocation and then grow through secondary allocations as more space is required for subsequent incremental updates. For example, enough space for one incremental update.

```

*
* Note: The INCRDETAIL and INCRDAYS parameters are
* required when you specify INCRDB DYNAM.
*

```

**INCRDETAIL**

-----

This statement is required if you specify either of these:

**INCRDB TAPE****INCRDB DYNAM**

Otherwise, this statement is optional. There is no default.

Specify this to define data set allocation parameters for the incremental update DETAIL data set (IUDETAIL):

**INCRDETAIL** data\_set\_allocation\_parameters

Note: INCRDETAIL is ignored when you specify INCRUPDATE NO.

The incremental update DETAIL data set (IUDETAIL) contains the current incremental update detail-level database files, and the DETAIL "to-date" data for the current daily update cycle. You should allocate DASD space equivalent to two cycles of this product's DETAIL timespan data.

If you specified INCRDB PERM (the default), your INCRDETAIL parameter specifications are used in generating the cccIUALC job (where ccc is the product ID).

- o You will execute the cccIUALC job to allocate and initialize the incremental update database and checkpoint files.
- o Omit the INCRDETAIL parameter if you prefer to specify data set allocation parameters directly in the generated prefix.MICS.CNTL(cccIUALC) job.

If you specified INCRDB TAPE or INCRDB DYNAM, your INCRDETAIL parameter specifications are used in incremental update DETAIL data set dynamic allocation during incremental update or DAILY job step execution.

- o The INCRDETAIL parameter is required for the TAPE or DYNAM option.
- o Specify data set allocation parameters, separated by blanks, according to SAS LIBNAME statement syntax. If you need multiple lines, repeat the INCRDETAIL keyword on the continuation line.

- o INCRDETAIL accepts the engine/host options documented in the SAS Companion for the z/OS Environment, including STORCLAS, UNIT, SPACE, BLKSIZE, DATACLAS, MGMTCLAS, and VOLSER.

Important! DO NOT SPECIFY THE DISP PARAMETER.

- o You can override the INCRDETAIL data set allocation parameters at execution-time using the //PARMOVRD facility. For more information about execution-time override of dynamic data set allocation parameters, see the PIOM, section 2.3.6.

Example 1:

```
INCRDETAIL STORCLAS=MICSTEMP SPACE=(xxxx,(pp,ss),,,ROUND)
```

where:

STORCLAS - specifies a storage class for a new data set.  
The name can have up to eight characters.

SPACE - specifies how much disk space to provide for a new data set being allocated, where:

xxxx is TRK, CYL, or blklen  
pp is the primary allocation  
ss is the secondary allocation

and ROUND specifies that the allocated space be "rounded" to a cylinder boundary when the unit specified was a block length. ROUND is ignored with the TRK or CYL options.

Example 2 (multiple lines):

```
INCRDETAIL STORCLAS=MICSTEMP UNIT=SYSDA
INCRDETAIL SPACE=(xxxx,(pp,ss),,,ROUND)
```

where:

STORCLAS - specifies a storage class for a new data set.  
The name can have up to eight characters.

UNIT - specifies the generic unit for a new data set.  
The name can have up to eight characters.

SPACE - specifies how much disk space to provide for

a new data set being allocated.

INCRDAYS

-----

This statement is required if you specify either of these:

INCRDB TAPE

INCRDB DYNAM

Otherwise, this statement is optional. There is no default.

Specify this to define data set allocation parameters for the incremental update DAYS data set (IUDAYS):

INCRDAYS        data\_set\_allocation\_parameters

Note: INCRDAYS is ignored when you specify INCRUPDATE NO.

The incremental update DAYS data set (IUDAYS) contains the current incremental update days-level database files, and the DAYS "to-date" data for the current daily update cycle. You should allocate DASD space equivalent to two cycles of this product's DAYS timespan data.

If you specified INCRDB PERM (the default), your INCRDAYS parameter specifications are used in generating the cccIUALC job (where ccc is the product ID).

- o You will execute the cccIUALC job to allocate and initialize the incremental update database and checkpoint files.
- o Omit the INCRDAYS parameter if you prefer to specify data set allocation parameters directly in the generated prefix.MICS.CNTL(cccIUALC) job.

If you specified INCRDB TAPE or INCRDB DYNAM, your INCRDAYS parameter specifications are used in incremental update DAYS data set dynamic allocation during incremental update or DAILY job step execution.

- o The INCRDAYS parameter is required for the TAPE or DYNAM option.
- o Specify data set allocation parameters, separated by

blanks, according to SAS LIBNAME statement syntax. If you need multiple lines, repeat the INCRDAYS keyword on the continuation line.

- o INCRDAYS accepts the engine/host options documented in the SAS Companion for the z/OS Environment, including STORCLAS, UNIT, SPACE, BLKSIZE, DATACLAS, MGMTCLAS, and VOLSER.

Important! DO NOT SPECIFY THE DISP PARAMETER.

- o You can override the INCRDAYS data set allocation parameters at execution-time using the //PARMOVRD facility. For more information about execution-time override of dynamic data set allocation parameters, see the PIOM, Section 2.3.6.

Example 1:

```
INCRDAYS STORCLAS=MICSTEMP SPACE=(xxxx,(pp,ss),,,ROUND)
```

where:

STORCLAS - specifies a storage class for a new data set.  
The name can have up to eight characters.

SPACE - specifies how much disk space to provide for a new data set being allocated, where:

xxxx is TRK, CYL, or blklen  
pp is the primary allocation  
ss is the secondary allocation

and ROUND specifies that the allocated space be "rounded" to a cylinder boundary when the unit specified was a block length. ROUND is ignored with the TRK or CYL options.

Example 2 (multiple lines):

```
INCRDAYS STORCLAS=MICSTEMP UNIT=SYSDA
INCRDAYS SPACE=(xxxx,(pp,ss),,,ROUND)
```

where:

STORCLAS - specifies a storage class for a new data set.  
The name can have up to eight characters.

UNIT - specifies the generic unit for a new data set.



The name can have up to eight characters.

SPACE - specifies how much disk space to provide for a new data set being allocated.

INCRCKPT  
-----

This statement is optional. Specify this to override default data set allocation parameters for the incremental update checkpoint data set:

INCRCKPT        data\_set\_allocation\_parameters

Note: INCRCKPT is ignored when you specify INCRUPDATE NO.

The incremental update checkpoint data set tracks incremental update job status and the data that has been processed during the current daily update cycle. The incremental update checkpoint is used to detect and block the input of duplicate data during incremental update processing. This data set will be exactly the same size as prefix.MICS.CHECKPT.DATA (the unit checkpoint data set), usually 20K to 200K depending on the prefix.MICS.PARMS(SITE) CKPTCNT parameter (100-9999).

Your INCRCKPT parameter specifications are used in generating the cccIUALC job (where ccc is the product ID).

- o You will execute the cccIUALC job to allocate and initialize the incremental update checkpoint file. If you specified INCRDB PERM, then the cccIUALC job will also allocate the incremental update DETAIL and DAYS database files.
- o By default the incremental update checkpoint data set is allocated as SPACE=(TRK,(5,2)) using the value you specified for the prefix.MICS.PARMS(JCLDEF) DASDUNIT parameter.
- o Omit the INCRCKPT parameter if you prefer to override data set allocation parameters directly in the generated prefix.MICS.CNTL(cccIUALC) job.

Specify data set allocation parameters, separated by blanks, according to SAS LIBNAME statement syntax. If you need multiple lines, repeat the INCRCKPT keyword on the

continuation line.

INCRCKPT accepts the engine/host options documented in the SAS Companion for the MVS Environment, including STORCLAS, UNIT, SPACE, BLKSIZE, DATACLAS, MGMTCLAS, and VOLSER.

Important! DO NOT SPECIFY THE DISP PARAMETER.

Example 1:

```
INCRCKPT STORCLAS=MICSTEMP SPACE=(xxxx,(pp,ss),,,ROUND)
```

where:

STORCLAS - specifies a storage class for a new data set.  
The name can have up to eight characters.

SPACE - specifies how much disk space to provide for  
a new data set being allocated, where:

xxxx is TRK, CYL, or blklen

pp is the primary allocation

ss is the secondary allocation

and ROUND specifies that the allocated space be  
"rounded" to a cylinder boundary when the unit  
specified was a block length. ROUND is ignored  
with the TRK or CYL options.

Example 2 (multiple lines):

```
INCRCKPT STORCLAS=MICSTEMP UNIT=SYSDA
INCRCKPT SPACE=(xxxx,(pp,ss),,,ROUND)
```

where:

STORCLAS - specifies a storage class for a new data set.  
The name can have up to eight characters.

UNIT - specifies the generic unit for a new data set.  
The name can have up to eight characters.

SPACE - specifies how much disk space to provide for  
a new data set being allocated.

## INCRSPLIT

-----

This statement is optional and defaults to this:

INCRSPLIT IGNORE

Specify the following if you want the incremental update job for this product to get input measurement data from the output of the SPLITSMF job. The optional `data_set_allocation_parameters` are used by the SPLITSMF job when creating the measurement data file for this product.

INCRSPLIT USE `data_set_allocation_parameters`

Note: INCRSPLIT is ignored when you specify INCRUPDATE NO.

This option would be used when multiple products in a single unit database are enabled to incremental update. The SPLITSMF job performs the same function for incremental update jobs as the DAILY job DAYSMF step performs for the DAYnnn database update steps.

- o The SPLITSMF job dynamically allocates, catalogs, and populates `prefix.MICS.ccc.IUSPLTDS` data sets for each product in the unit database for which you specified both the INCRUPDATE YES and INCRSPLIT USE parameters. These data sets are then deleted after processing by the appropriate INCRccc job.
- o Specify data set allocation parameters, separated by blanks, according to SAS LIBNAME statement syntax. If you need multiple lines, repeat the INCRSPLIT keyword on each continuation line.
- o INCRSPLIT accepts the engine/host options documented in the SAS Companion for the MVS Environment, including STORCLAS, UNIT, SPACE, BLKSIZE, DATACLAS, MGMTCLAS, and VOLSER.

Important! DO NOT SPECIFY THE DISP PARAMETER.

Specify the following or accept the default if you want the incremental update jobs for this product to get their input measurement data from the data sets specified in the INPUTccc (or INPUTSMF) member of `prefix.MICS.PARMS`:

INCRSPLIT IGNORE

When you specify INCRSPLIT IGNORE, this product will NOT participate in SPLITSMF job processing.

Example 1:

INCRSPLIT USE STORCLAS=MICSTEMP SPACE=(xxxx,(pp,ss),,,ROUND)

where:

STORCLAS - specifies a storage class for a new data set.  
The name can have up to eight characters.

SPACE - specifies how much disk space to provide for  
a new data set being allocated, where:

xxxx is TRK, CYL, or blklen  
pp is the primary allocation  
ss is the secondary allocation

and ROUND specifies that the allocated space be  
"rounded" to a cylinder boundary when the unit  
specified was a block length. ROUND is ignored  
with the TRK or CYL options.

Example 2 (multiple lines):

INCRSPLIT USE STORCLAS=MICSTEMP UNIT=SYSDA  
INCRSPLIT SPACE=(xxxx,(pp,ss),,,ROUND)

where:

STORCLAS - specifies a storage class for a new data set.  
The name can have up to eight characters.

UNIT - specifies the generic unit for a new data set.  
The name can have up to eight characters.

SPACE - specifies how much disk space to provide for  
a new data set being allocated.

DYNAMWAIT

-----

This statement is optional. Specify the following:

DYNAMWAIT minutes

to override the default amount of time, in minutes, the DAILY and/or INCRccc job will wait for an unavailable data set.

Note: This optional parameter is not normally specified.  
The system default is adequate for most data centers.

Internal Step Restart and Incremental Update facilities use z/OS dynamic allocation services to create new data sets and to access existing data sets. Data set naming conventions and internal program structure are designed to minimize data set contention. However, if data set allocation does fail because another batch job or online user is already using a data set, DAILY and/or INCRccc processing will wait 15 seconds and then try the allocation again. By default, the allocation will be attempted every 15 seconds for up to 15 minutes. After 15 minutes, the DAILY or INCRccc job will abort.

If data set contention in your data center does cause frequent DAILY or INCRccc job failures, and you are unable to resolve the contention through scheduling changes, you may want to use the DYNAMWAIT parameter to increase the maximum number of minutes the DAILY and/or INCRccc jobs will wait for the data set to become available.

On the other hand, if your data center standards require that the DAILY and/or INCRccc jobs fail immediately if required data sets are unavailable, specify the following:

DYNAMWAIT 0

Note: You can override the DYNAMWAIT parameter at execution-time using the //PARMOVRD facility. For more information about execution-time override of dynamic data set allocation parameters, see the PIOM, section 2.3.6.

The following section discusses enabling this option:

#### 1 - Implement Incremental Update

### 7.3.1.14.1 Implement Incremental Update

To implement incremental update in the CA MICS Network Analyzer, follow the checklist provided below:

```

* *
* IMPLEMENT INCREMENTAL UPDATE *
* *

```

- \_\_\_ 1. Edit prefix.MICS.PARMS(cccOPS), where (ccc) is the component identifier:
  - o Specify the following:  
  
INCRUPDATE YES
  - o If you want to store the incremental update database files on tape between incremental updates, specify this:  
  
INCRDB TAPE #gdgs
  - o If you want to allocate the incremental update database files during the first incremental update of the day and delete these data sets at the end of the DAILY job step, specify this:  
  
INCRDB DYNAM
  - o If you specified INCRDB TAPE or INCRDB DYNAM, then you must also specify this:  
  
INCRDETAIL data\_set\_allocation\_parameters  
INCRDAYS data\_set\_allocation\_parameters
  - o If you want the incremental update job for this product to get input measurement data from the output of the SPLITSMF job, specify this:  
  
INCRSPLIT USE data\_set\_allocation\_parameters
  - o For additional information on related topic, review the documentation for this product on INCRCKPT, INCRDETAIL, INCRDAYS, or INCRSPLIT parameters to override default data set allocation parameters.

- \_\_\_ 2. Submit the job in prefix.MICS.CNTL(cccPGEN).
- \_\_\_ 3. Edit prefix.MICS.PARMS(JCLGENU) so that it contains two or more lines reading:  
  
DAILY  
INCRccc cccIUALC cccIUGDG
- \_\_\_ 4. Submit the job in prefix.MICS.CNTL(JCLGENU). Ensure that there are no error messages in MICSLOG or SYSTSPRT, that the MICSLOG contains the normal termination message, BAS10999I, and that the job completes with a condition code of zero.
- \_\_\_ 5. Edit the job in prefix.MICS.CNTL(cccIUALC).
  - o Inspect and/or specify data set allocation parameters for the incremental update database and checkpoint files. If you specified INCRDB TAPE or INCRDB DYNAM, the cccIUALC job will only allocate the incremental update checkpoint data set.
  - o Submit the job. Ensure that there are no error messages in MICSLOG or SASLOG, and that the job completes with a condition code of zero.
- \_\_\_ 6. If you specified INCRDB TAPE, submit the job in prefix.MICS.CNTL(cccIUGDG) to define generation group indexes for the incremental update DETAIL and DAYS tape data sets. Examine SASLOG, MICSLOG, and SYSPRINT to verify that the generation group indexes were correctly defined.

Note: You may see error messages for the DLTX (or DELETE) statements. This is not a problem. cccIUGDG deletes each index prior to defining it, and an error message is issued if the index does not yet exist (e.g., if this is the first time you ran the cccIUGDG job).

- \_\_\_ 7. The following operational job(s) have changed:

DAILY INCRccc

If your site has implemented the operational CA MICS processes in a scheduling product, the JCL may have to be refreshed in that product. See the scheduling product's administrator for the exact processes

involved in updating that product's representation of the CA MICS jobs.

- \_\_\_ 8. Implement operational procedures for gathering input measurement data and executing incremental updates (INCRccc) during the day.

You may also need to modify operational procedures for the DAILY job to ensure that processing is limited to input measurement data that has not been input to one of the day's incremental update executions.



### 7.3.1.15 DETAIL Tape Processing Overview

For certain high volume files, the CA MICS architecture provides the ability to create optional DETAIL timespan data sets. These optional data sets are separate from the normal CA MICS database and have the following characteristics:

- o They are created during the component step execution: during either an incremental update or the DAILY update run. Each DETAIL tape file has a separate DD statement in the DAILY or incremental update job that specifies the data set name and other data set characteristics.
- o The data set name (DSN) for each DETAIL tape in a component step is:

tapeprefix.tmics.DETAIL.iiiiff(+1)

where:

- tapeprefix is the tape prefix value specified with the TAPEPREFIX statement in prefix.MICS.PARMS(JCLDEF)
- tmics is either null when NOMICSLEVEL is specified, or MICS if MICSLEVEL is specified with the TAPEPREFIX statement in prefix.MICS.PARMS(JCLDEF)
- iii is the three character CA MICS information area associated with the file
- fff is the three character CA MICS file identifier

Example: For the CA MICS DB2 Analyzer, if DETAIL tape processing were activated for the DB2DSU file, the following prefix.MICS.PARMS(JCLDEF) statement:

TAPEPREFIX CPLXA.U1T NOMICSLEVEL

yields the following DETAIL tape DSN:

CPLXA.U1T.DETAIL.DB2DSU(+1)

- o There is no cycle aging associated with these data sets. Instead, each DETAIL tape data set created is an 01 cycle (for example, DB2DSU01), and multiple instances are managed using Generation Data Groups (GDGs).

- o The creation of DETAIL tape data sets is independent of any sharedprefix.MICS.GENLIB customization choices. You can have one or more cycles of a file written to and managed in the unit DETAIL timespan database, and also use the DETAIL tape feature to create independent data sets for that same file.
- o The decision to create DETAIL tape data sets is made at the unit level. You can choose to create DETAIL tape data sets for a component file in unit A, but not in unit B.
- o While the expectation is that these files will be written to tape, you can make JCL choices to target other media such as DASD. Note that the SAS sequential tape engine will be used to write these files for both DASD and tape data sets.
- o Unique output exits are provided to permit manipulation and subsetting of the records written to the DETAIL tape data sets. This manipulation and subsetting, however, has no impact on files written to the standard CA MICS database.

The activation of DETAIL tape data sets is accomplished by specifying a TAPEfff statement in prefix.MICS.PARMS(cccOPS).

Customization of the JCL used to create each data set is accomplished using a cascading hierarchy of parameters beginning with choices made with the TAPEPARM statement in prefix.PARMS(JCLDEF).

The following sections provide the information required to activate DETAIL tape processing:

- 1 - Component Files Supporting DETAIL Tape Activation
- 2 - DETAIL Tape JCL Customization Overview
- 3 - The TAPEfff Statement
- 4 - The DETAILTAPEPARM Statement
- 5 - DETAILTAPESMSPARM and TAPEfffSMS Statements
- 6 - DETAIL Tape User Exits
- 7 - Activating DETAIL Tape Checklist
- 8 - Deactivating DETAIL Tape Checklist

#### 7.3.1.15.1 SNT DETAIL Tape Supported Files

The CA MICS Network Analyzer supports DETAIL tape processing for the following file:

- o TCPAPI - API Calls for Sockets File

### 7.3.1.15.2 Overview of JCL Customization Parameters

The JCL for DETAIL tape data sets is constructed using tape-related parameters that are specified in `prefix.MICS.PARMS(JCLDEF)` and `prefix.MICS.PARMS(cccOPS)`.

Each DETAIL tape data set has a unique DD in the component step. The JCL for each DETAIL tape data set is customized according to user-specified JCL parameters such as the number of generation data group (GDG) entries that are maintained, unit names, volume count, retention, and expiration dates, and System Managed Storage (SMS) keywords. For example, `STORCLAS=storclas`.

CA MICS provides a hierarchical means to specify tape-related JCL parameters suitable for each data center.

The hierarchy, as it applies to DETAIL tape specification, is described:

- o Unit Level - `TAPEPARM` and `TAPESMSPARM`

Used for all tape data sets created by all components in the unit. Specified in `prefix.MICS.PARMS(JCLDEF)`

- o Unit DETAIL Tape Level - `DETAILTAPEPARM` and `DETAILTAPESMSPARM`

Used for all DETAIL tape data sets created by all components in the unit. Overrides choices that were made in `TAPEPARM` and `TAPESMSPARM`. Specified in `prefix.MICS.PARMS(JCLDEF)`.

- o Component Level - `DETAILTAPEPARM` and `DETAILTAPESMSPARM`

Used for all DETAIL tape data sets created by a particular component. Overrides all choices that were made in `JCLDEF`. Specified in `prefix.MICS.PARMS(cccOPS)`, where `ccc` represents the component.

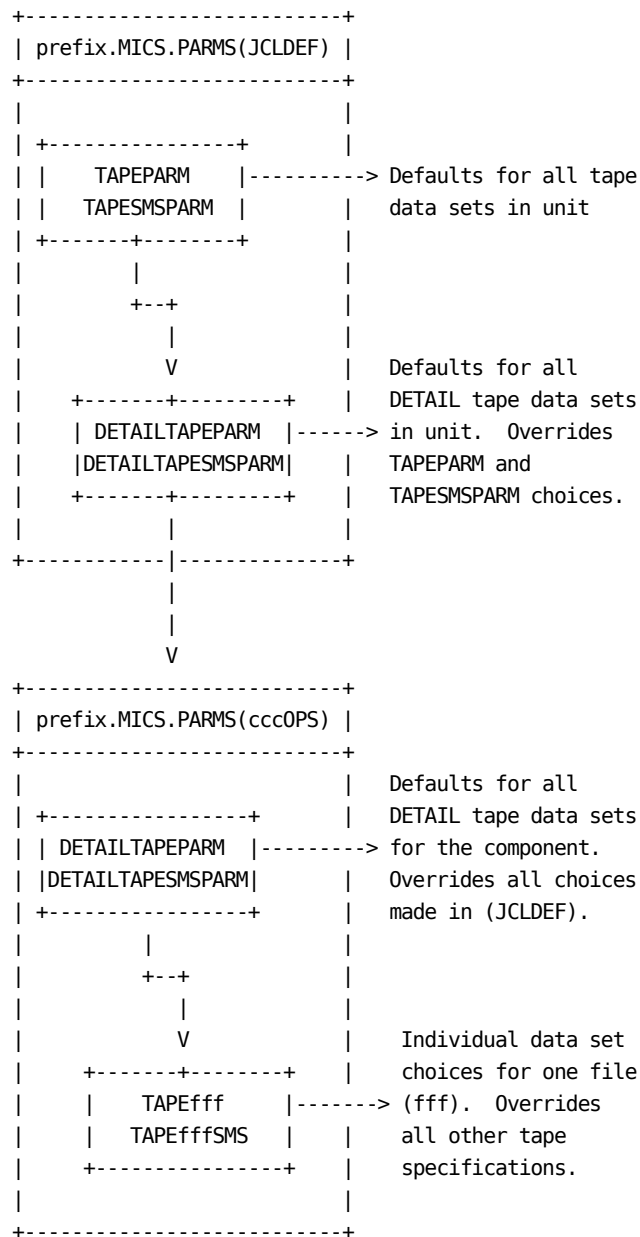
- o File Level - `TAPEfff` and `TAPEfffsMS`

Used for a particular DETAIL tape data set. The `fff` identifies the specific DETAIL file. Overrides all choices made in `JCLDEF` and choices that were made with `DETAILTAPEPARM` and `DETAILTAPESMSPARM` in `prefix.MICS.PARMS(cccOPS)`. Specified in `prefix.MICS.PARMS(cccOPS)`, where `ccc` represents the

component.

The JCL parameter specification hierarchy that is used for DETAIL tape customization is shown graphically in the following diagram:

DETAIL Tape JCL Parameter Hierarchy



I  
V

// DD statements and GDG generation

### 7.3.1.15.3 The TAPEfff Statement

The TAPEfff statement is used to:

- o Activate DETAIL tape data set creation for the file indicated by fff. The component files eligible for DETAIL tape processing are listed in a previous section.
- o Override, for the indicated file, any JCL-related tape specifications made in prefix.MICS.PARMS(JCLDEF) and prefix.MICS.PARMS(cccOPS) with TAPEPARM or DETAILTAPEPARM statements.

The syntax is as follows:

TAPEfff <optional parameters>

where fff is the unique 3-character file identifier

The optional parameters include both keyword parameters and keyword=value specifications. You can include multiple TAPEfff statements if required in order to specify the desired optional parameters. If you specify a parameter multiple times, the last instance defines the value in effect.

You can specify as many parameters as you want on each statement, but each TAPEfff statement must end by column 72. You may also choose to specify only one parameter per TAPEfff statement. Either approach is acceptable.

The optional parameters available for the TAPEfff statement are listed below:

```
TAPEfff GDG=nnn UNIT=unitname VOLCOUNT=n
TAPEfff EXPDT=expdt / RETPD=nnn / NOEXPDT
TAPEfff COMP/NOCOMP
TAPEfff STACK/NOSTACK AFF/NOAFF
TAPEfff MODEL='modeldsn' / MODEL=NOMODEL
TAPEfff DISK / TAPE SPACE=spacedef
TAPEfff VOLSER=volser
```

The following is a sample TAPEfff statement:

```
TAPEfff GDG=3 VOLCOUNT=7
```

In this sample, only the number of generation data groups (GDGs) and VOLCOUNT parameters are explicitly specified for

the file fff. All other JCL related parameters for the data set will be set according to specifications made with TAPEPARM and DETAILTAPEPARM statements according to the hierarchy described in a previous section.

The optional parameters for the TAPEfff statement are identical to those supported by the DETAILTAPEPARM statement. A detailed description of the optional parameters is presented immediately following the DETAILTAPEPARM statement description.



#### 7.3.1.15.4 The DETAILTAPEPARM Statement

In `prefix.MICS.PARMS(cccOPS)`, the optional DETAILTAPEPARM statement is used to specify parameters defining processing options for CA MICS DETAIL tape data sets at the component (ccc) level.

When specified in `prefix.MICS.PARMS(cccOPS)`, the DETAILTAPEPARM parameter specifications override unit level tape data set defaults established by TAPEPARM and DETAILTAPEPARM statements in `prefix.MICS.PARMS(JCLDEF)`.

Refer to chapter 2 of the CA MICS Planning, Installation, Operations, and Maintenance Guide for unit level TAPEPARM and DETAILTAPEPARM statements in `prefix.MICS.PARMS(JCLDEF)`.

The primary reason to include a DETAILTAPEPARM statement in `prefix.MICS.PARMS(cccOPS)` is to specify unique parameters for the DETAIL tapes created for a particular component (ccc).

For example, your site may want to direct the CA MICS DETAIL tapes for a particular component (ccc) to a unique tape volume pool, or to a tape device type such as a virtual tape unit, or to a DASD pool backed by an archive facility. If so, this could be accomplished by including the appropriate DETAILTAPEPARM statements in `prefix.MICS.PARMS(cccOPS)`.

DETAILTAPEPARM <parameters>

Note: In `prefix.MICS.PARMS(cccOPS)`, all DETAILTAPEPARM statements must precede any TAPEfff or TAPEfffsms statements.

The general form of the DETAILTAPEPARM statement is the keyword DETAILTAPEPARM, followed by one or more DETAILTAPEPARM parameters. DETAILTAPEPARM parameters include both keyword parameters and keyword=value specifications. You can specify the DETAILTAPEPARM statement as many times as you want in order to specify all of the tape data set definitions you require. If you specify a parameter multiple times, the last instance defines the value in effect.

The following summarizes the DETAILTAPEPARM parameters:

- o Each parameter is described in detail below.
- o While the following syntax sample shows only one or

two parameters per statement (line), you have the option to specify as many parameters as you want on each statement (limited only by the 72-character-maximum line length).

```
DETAILTAPARM GDG=nnn UNIT=unitname VOLCOUNT=n
DETAILTAPARM EXPDT=expdt / RETPD=nnn / NOEXPDT
DETAILTAPARM COMP/NOCOMP
DETAILTAPARM STACK/NOSTACK AFF/NOAFF
DETAILTAPARM MODEL='modeldsn' / MODEL=NOMODEL
DETAILTAPARM DISK / TAPE SPACE=spacedef
DETAILTAPARM VOLSER=volser
```

The following is a sample DETAILTAPARM statement:

```
DETAILTAPARM GDG=3 VOLCOUNT=7
```

In this example, the default parameter values are used for most of the DETAILTAPARM parameters.

The following describes each of the DETAILTAPARM parameters:

- o GDG=nnn

Defaults to 7.

The number of entries to be created in the GDG for each DETAIL tape data set.

Overrides the TAPARM statement GDG=nnn.

- o UNIT=unitname

Defaults to the value specified on the TAPARM statement or to UNIT=3490 if UNIT=unitname is not specified on the TAPARM statement.

The generic unit name for tape file allocation. The parameter value (unitname) must be a valid 1 to 8 character generic unit name for your installation. The value will be used in generated tape data set JCL DD statement UNIT parameters. CA MICS does not validate the unitname value except to verify that it is non-blank and no more than 8 characters in length.

Overrides the TAPEPARM statement UNIT=unitname Value, the old-style TAPEUNIT statement, or both.

o VOLCOUNT=n

Defaults to the value specified on the TAPEPARM statement. If no VOLCOUNT is specified, the z/OS default volume count of 5 applies.

The volume count JCL parameter for CA MICS tape data sets. Specify a decimal number from 1 to 255.

Overrides the TAPEPARM statement VOLCOUNT=nnn parameter or the old-style VOLCOUNT statement.

o EXPDT=expdt

Defaults to the value specified on the TAPEPARM statement. If no expiration date or retention period is specified, a default retention period is used which equals the GDG=nnn value.

Specify an expiration date definition which replaces the derived default retention period (RETPD) specifications. This facility is specifically intended for use by installations with tape management systems which require specific EXPDT definitions.

Note: For some tape management systems, certain EXPDT values makes the tape available for scratching immediately. Such values are NOT suitable for CA MICS tapes.

The EXPDT=expdt parameter is optional, and, if omitted, CA MICS derives a RETPD=nnn specification as appropriate for the specific CA MICS tape data set being created and the number of GDG entries defined.

Overrides the TAPEPARM statement EXPDT=expdt or NOEXPDT parameter, or the old-style EXPDT statement.

Note: The EXPDT=expdt, RETPD=nnn, and NOEXPDT parameters are mutually exclusive.

- o NOEXPDT

Defaults to the value specified on the TAPEPARM statement.

Specify NOEXPDT if you want CA MICS to omit both the EXPDT=date and RETPD=days JCL parameters from generated JCL statements for new tape data set creation. This option is provided for those installations where the tape management system or SMS specifications automatically control tape expiration dates, retention periods, or both.

Overrides the TAPEPARM statement EXPDT=expdt or NOEXPDT parameters, or the old-style EXPDT statement.

Note: The NOEXPDT, EXPDT=expdt, and RETPD=nnn parameters are mutually exclusive.

- o COMP / NOCOMP

Defaults to the value specified on the TAPEPARM statement. If COMP or NOCOMP is not specified, the z/OS default for the selected tape unit type applies.

This parameter specifies data compaction (COMP) or no data compaction (NOCOMP) for a tape device enabled for hardware compaction. Data compaction is only supported for IBM standard labels. If specified, the value will be coded in the TRTCH subparameter of the DCB JCL parameter. If not specified, no TRTCH subparameter will be generated.

Overrides the TAPEPARM statement COMP/NOCOMP parameter or the old-style IDRC statement.

- o STACK / NOSTACK

Defaults to NOSTACK for DETAIL tapes.

Specify STACK to place multiple CA MICS tape files on a single tape volume. This mode of operation uses a minimum number of tape volumes and tape mounts are minimized. CA MICS

JCL statements are generated with the VOL=REF=ddname construct and unit affinity is enforced (that is, STACK also means AFF).

Specify NOSTACK (the default) to place exactly one CA MICS tape file on a tape volume. With this option the generated CA MICS JCL statements will NOT contain the VOL=REF=ddname construct. This option is useful if your implementation of a virtual tape system prohibits "stacked" tape volumes, or if you are directing CA MICS tape files to a DASD pool backed with an archival facility.

Overrides the TAPEPARM statement STACK/NOSTACK parameter.

o AFF / NOAFF

Defaults to the value specified on the TAPEPARM statement or to AFF.

Specify AFF to use a single tape unit for all related tape files. This is the normal mode of operation where a minimum number of tape units are used and tape mounts are minimized. CA MICS JCL statements are generated with the UNIT=AFF=ddname construct. AFF is required for the STACK option.

Specify NOAFF to enable allocation of different tape units for each CA MICS tape data set. With this option the generated CA MICS JCL statements will NOT contain the UNIT=AFF=ddname construct. You may find this option useful with certain virtual tape system implementations, or where you are directing CA MICS tape files to a DASD pool backed with an archival facility.

Note, if you specify NOAFF, then NOSTACK is automatically set.

Overrides the TAPEPARM statement AFF/NOAFF parameter.

o MODEL='modeldsn' / MODEL=NOMODEL

Defaults to the value specified on the TAPEPARM statement.

The fully qualified name of a cataloged data set to be used when defining or extending GDG entries. Ensure that the data set's DCB characteristics are LRECL=0 and BLKSIZE=0. Coding BLKSIZE=0 causes SAS to use the blocksize defined by the BLKSIZE(TAPE) option defined in the configuration member(s) referenced by the CONFIG DD statement. If this parameter is omitted, a CA MICS generation job will allocate a default model GDG data set.

If NOMODEL is specified as the model dataset name, the use of the model dataset in the DCB specification will be bypassed.

Overrides the TAPEPARM statement MODEL='modeldsn' parameter or the old-style SYSTEMMODEL statement.

- o DISK / TAPE

Defaults to TAPE.

Specify DISK if you want to write the dataset to a disk instead of a tape. Specify TAPE to write the dataset to a tape.

When you specify DISK, make sure that you have both a UNIT parameter with a generic unit name of a disk device and a SPACE parameter defining disk space. You can also define a VOLSER parameter to direct the data to a specific disk.

Overrides the TAPEPARM statement DISK/TAPE parameter.

- o SPACE=spacedef

No default.

Defines the space allocation parameter for a data set defined with the DISK parameter. Specify this parameter according to JCL language syntax.

Overrides the TAPEPARM statement SPACE= parameter.

- o VOLSER=volser

No default.

Defines the volume serial number of a disk for a

data set defined with the DISK parameter. Specify this parameter according to JCL language syntax.

Overrides the TAPEPARM statement VOLSER= parameter.

### 7.3.1.15.5 DETAILTAPESMSPARM and TAPEfffsSMS Statements

In `prefix.MICS.PARMS(cccOPS)`, the optional `DETAILTAPESMSPARM` and `TAPEfffsSMS` statements allow you to specify System Managed Storage (SMS) keywords (for example, `STORCLAS=storclass`) for `DETAIL` tape data sets at the component and individual file level, respectively.

#### DETAILTAPESMSPARM

When specified in `prefix.MICS.PARMS(cccOPS)`, the `DETAILTAPESMSPARM` parameter specifications override unit level tape data set SMS defaults established by `TAPESMSPARM` and `DETAILTAPESMSPARM` statements in `prefix.MICS.PARMS(JCLDEF)`.

Refer to chapter 2 of the CA MICS Planning, Installation, Operations, and Maintenance Guide for unit level `TAPESMSPARM` and `DETAILTAPESMSPARM` statements in `prefix.MICS.PARMS(JCLDEF)`.

The primary reason to include a `DETAILTAPESMSPARM` statement in `prefix.MICS.PARMS(cccOPS)` is to specify unique SMS parameters for the `DETAIL` tapes created for a particular component (`ccc`).

For example, your site may want to direct the CA MICS `DETAIL` tapes for a particular component (`ccc`) to a unique storage class.

Sample `DETAILTAPESMSPARM` statement:

```
DETAILTAPESMSPARM STORCLAS=DTPCLASS
```

In this example, the JCL for all `DETAIL` tape data sets for the component will include the SMS `STORCLAS=DTPCLASS` assignment.

#### TAPEfffsSMS

The `TAPEfffsSMS` statement is only permitted in `prefix.MICS.PARMS(cccOPS)`. It is not supported in `prefix.MICS.PARMS(JCLDEF)`. `TAPEfffsSMS` keyword specifications override, for the indicated file, any SMS related tape specifications made in `prefix.MICS.PARMS(JCLDEF)` and `prefix.MICS.PARMS(cccOPS)` with `TAPESMSPARM` or `DETAILTAPESMSPARM` statements.



The primary reason to include a `TAPEfffSMS` statement in `prefix.MICS.PARMS(cccOPS)` is to specify unique SMS parameters for a specific DETAIL tape file (fff).

Sample `TAPEfffSMS` statement:

```
TAPEfffSMS STORCLAS=fffCLASS
```

In this example, the JCL for the DETAIL tape data set for file `ffft` will include the SMS `STORCLAS=fffCLASS` assignment.

#### 7.3.1.15.6 DETAIL Tape User Exits

A user exit is invoked just prior to the output of each record to a DETAIL tape file. The exits are named `_USRTfff`, where `fff` matches the file identifier for the DETAIL tape file.

Refer to chapter 10 of this guide for a complete description of the DETAIL tape user exits.

### 7.3.1.15.7 Activating DETAIL Tape Checklist

- \_\_\_ 1. Add or modify the desired TAPEfff and TAPEfffsms statements in prefix.MICS.PARMS(cccOPS), where fff is the three-character file identifier for the file to be written to tape.

- \_\_\_ 2. Submit prefix.MICS.CNTL(cccPGEN).

- \_\_\_ 3. Edit prefix.MICS.PARMS(JCLGENU) so that it reads:

cccGDGDN DAILY

If Incremental Update is active, add this:

INCRccc

- \_\_\_ 4. Submit prefix.MICS.CNTL(JCLGENU) to regenerate the JCL for DAILY and cccGDGDN.

Note: If you want to use specific JCL and SMS parameter values for your DETAIL tape data sets, make sure you have coded the appropriate DETAILTAPEPARM and/or DETAILTAPESMSPARM statements in prefix.MICS.PARMS(JCLDEF) for unit level, or prefix.MICS.PARMS(cccOPS) for component level DETAIL tape JCL parameters. Refer to the previous sections for a detailed discussion on JCL parameters available for DETAIL tape data sets.

- \_\_\_ 5. Submit prefix.MICS.CNTL(cccGDGDN) to define the tape GDG.

Note: If you want to override the number of entries kept in a GDG with cataloged data sets for a TAPEfff file, you must delete and redefine the index with the new limit for GDG entries. Follow the checklist in section 3.5.6.3 of the PIOM.

- \_\_\_ 6. You have just activated DETAIL tape for one or more database files. As mentioned in the DETAIL Tape Processing Overview section, the choice to create DETAIL tape files is independent of, and does not affect the creation of DETAIL files in the unit database.

If you are currently creating one or more cycles of the files you just activated for DETAIL tape in your

unit prefix.MICS.DETAIL timespan, your DAILY update job will continue to do so.

Now that you are creating DETAIL tape cycles for the files, you may want to deactivate, or limit the number of DETAIL cycles written to the unit DETAIL timespan database.

The CA MICS System Modification Guide contains instructions for changing the number of cycles of a file as well as instructions for deactivation of the DETAIL timespan of a file.

If you deactivate the files in the DETAIL timespan, make sure you delete the existing cycles to free up space in the prefix.MICS.DETAIL database. If you reduce the number of cycles, make sure you delete any existing cycles in prefix.MICS.DETAIL beyond the new cycle limit.

The following JCL can be used to delete specific cycles of a file from the DETAIL timespan. Make sure to replace 'x' with the unit identifier:

a) Delete all cycles for file fff (01-nn)

```
//DELETE EXEC MICSDBx
//SYSIN DD *
PROC DATASETS DDNAME=%DDNx(TS=DETAIL);
 DELETE cccfff01 cccfff02 ... cccfffn ;
RUN;
```

b) Delete cycles 02, 03, and 04 for file fff:

```
//DELETE EXEC MICSDBx
//SYSIN DD *
PROC DATASETS DDNAME=%DDNx(TS=DETAIL);
 DELETE cccfff02 cccfff03 cccfff04 ;
RUN;
```

### 7.3.1.15.8 Deactivating DETAIL Tape Checklist

- \_\_\_ 1. Delete the desired TAPEfff and TAPEfffsMS statements from prefix.MICS.PARMS(cccOPS).
- \_\_\_ 2. If there are no longer any TAPEfff statements in prefix.MICS.PARMS(cccOPS), delete any DETAILTAPEPARM and DETAILTAPEMSPARM statements.
- \_\_\_ 3. Submit prefix.MICS.CNTL(cccPGEN).
- \_\_\_ 4. Edit prefix.MICS.PARMS(JCLGENU) so that it reads:  
  
DAILY  
  
If Incremental Update is active, add this:  
  
INCRccc
- \_\_\_ 5. Submit prefix.MICS.CNTL(JCLGENU) to regenerate the JCL for the DAILY job.
- \_\_\_ 6. (Optional) Delete the index and the cataloged datasets for each TAPEfff statements deleted in step 1.

## 7.3.1.16 Sample SNTOPS

Following is a sample of required and optional statements that may be coded in prefix.MICS.PARMS(SNTOPS).

```
+-----+
| INSTALLATION PREPARATION WORKSHEET: CA MICS Network Analyzer Options Def. |
| PARMS Library Member is SNTOPS |
+-----+
| SNTNAC SUSPEND ____ NVSNSC SUSPEND ____ TCP SUSPEND ____ |
| |
| NETWORK ID _____ |
| ORGSYSID _____ |
| TIME OFFSET _____ |
| |
| DATA SOURCES ____ (NLDM) ____ (NPDA) ____ (NPMN) ____ (NPMS) ____ (NSPY) |
| |
| ____ (NTS) ____ (NEWS) ____ (NTRI) ____ (TIC3) ____ (X25) ____ (GENA/ |
| |
| DELETEMS YES ____ NO ____ |
| |
| ORGSYSID _____ |
| TIME OFFSET _____ |
| |
| DATA SOURCES ____ (NLDM) ____ (NPDA) ____ (NPMN) ____ (NPMS) ____ (NSPY) |
| |
| ____ (NTS) ____ (NEWS) ____ (NTRI) ____ (TIC3) ____ (X25) ____ (GENA/ |
| |
| DELETEMS YES ____ NO ____ |
| |
| NETWORK ID _____ |
| ORGSYSID _____ |
| TIME OFFSET _____ |
| |
| DATA SOURCES ____ (NLDM) ____ (NPDA) ____ (NPMN) ____ (NPMS) ____ (NSPY) |
| |
| _ (NTCP) _ (NTS) _ (NEWS) _ (NTRI) _ (TIC3) _ (X25) _ (GENA/ |
| |
| NETSPY SMF = nnn |
| NETTCP SMF = nnn |
| DELETEMS YES ____ NO ____ |
| |
| WORK n data_set_allocation_parameters |
| MULTWORK|NOMULT fff ... fff |
| |
| RESTART YES/NO |
| |
| INCRUPDATE YES/NO |
| INCRDB PERM/TAPE/DYNAM |
| INCRDETAIL data_set_allocation_parameters |
| |
```

```
+-----+
| ...5...10...15...20...25...30...35...40...45...50...55...60...65...70.. |
+-----+
```

Figure 7-4. CA MICS Network Analyzer Options Definition Worksheet

## 7.3.2 INPUTRDR and INPUTSNT PARMS Members

The prefix.MICS.PARMS members INPUTRDR and INPUTccc are used to specify the input data for the Data Integration Application component step.

To determine whether INPUTccc or INPUTRDR or both are used, review the DAYSMF, SMFRECORDING, and SMFDRCRTR specifications in prefix.MICS.PARMS(JCLDEF). Consider the following table and comments for the row:

| ROW | PARAMETER<br>IN JCLDEF | INPUTRDR<br>WHERE USED | INPUTccc<br>WHERE USED |
|-----|------------------------|------------------------|------------------------|
| 1   | DAYSMF OFF             | Not Used               | Each Comp Step         |
| 2   | DAYSMF FILE(S) ...     | DAYSMF Step            | Not Used               |
| 3   | Only 1 SMF Comp        | Comp Step              | Not Used               |
| 4   | SMFDIRECTOR            | Not Used               | Comp Step              |
| 5   | DAYSMF EXCLUDE ccc     | Not Used               | Comp ccc Step          |
| 6   | SMFRECORDING ccc       | It depends             | Comp ccc Step          |

Row 1: When DAYSMF OFF is specified in JCLDEF, then the prefix.MICS.PARMS(INPUTccc) member is used for each component step.

Row 2: When DAYSMF FILES PERMANENT or TEMPORARY is specified in JCLDEF, the prefix.MICS.PARMS(INPUTRDR) member is used in DAYSMF.

Row 3: If there is only one SMF recording component in this unit, DAYSMF will not be generated and the component step with SMF input data will use the prefix.MICS.PARMS(INPUTRDR) member.

Row 5: If the use of DAYSMF EXCLUDE ccc results in only one component remaining as DAYSMF eligible, DAYSMF will automatically be deactivated, and row 1 applies.

Row 6: Some components accept data from both SMF and non-SMF sources, such as CIC and VCA. In this case, the component may optionally input data from the INPUTRDR member, but will always include the INPUTccc member. Refer to the component's guide.

For details on the DAYSMF parameters, see PIOM section 2.3.3.2.1, JCL Option Definitions (JCLDEF).

For details on deactivating DAYSMF, see PIOM section 5.10, Removing the DAYSMF Step from the DAILY Job.

The following sections describe how to specify the input data set JCL definitions.

- 1 - INPUTRDR PARMs Member JCL Definition
- 2 - INPUTSNT PARMs Member JCL Definition



### 7.3.2.1 INPUTRDR PARMS Member JCL Definition

The INPUTRDR member of prefix.MICS.PARMS defines the DD statements that specify the SMF input data for all products in the units that use SMF data. The INPUTSMF DD statements are used by the DAYSMF step, which reads and splits the SMF data into separate files, one for each CA MICS product.

The INPUTRDR member defines the input SMF data sets when DAYSMF FILES PERMANENT or TEMPORARY is specified in the prefix.MICS.PARMS(JCLDEF) member.

An INPUTSMF DD statement is required for each SMF data source. A worksheet for preparing the INPUTRDR member is provided below. If you change the contents of the INPUTRDR member, you must regenerate the CA MICS DAILY job using either JCLGENU or JCLGEN in prefix.MICS.CNTL.

For example, if you want to read your SMF data from a data set named SMF.DAILY.DATA, you would change the INPUTRDR member to contain the name of the SMF data set as follows:

```
//INPUTSMF DD DISP=SHR,DSN=SMF.DAILY.DATA
```

If there is only one SMF recording component in this unit, DAYSMF will not be generated and the component step with SMF input data will use the prefix.MICS.PARMS(INPUTRDR) member directly.

If DAYSMF has been deactivated by the DAYSMF OFF statement specified in the prefix.MICS.PARMS(JCLDEF) member, then each component step will read its input from their corresponding prefix.MICS.PARMS(INPUTccc) member.

```
+-----+
| INSTALLATION PREPARATION WORKSHEET: SMF Input DD
Statements |
|
| PARMS Library Member is INPUTRDR
|
+-----+
|
| This definition is required to specify the DD statement
for SMF data |
```

|                                |  |                                                     |  |
|--------------------------------|--|-----------------------------------------------------|--|
|                                |  | which will be read by the DAILY CA MICS job.        |  |
|                                |  |                                                     |  |
|                                |  | //@                                                 |  |
|                                |  | //@ WARNING: ALWAYS MAKE CHANGES IN PARMs(INPUTRDR) |  |
| AND NOT                        |  | //@ &CNTL(DAILY).                                   |  |
|                                |  | //@ CHANGES MADE TO &CNTL(DAILY)                    |  |
|                                |  | //@ WILL BE GONE WHEN DAILY REGENERATED BY          |  |
| JCLGEN.                        |  | //@                                                 |  |
|                                |  | //INPUTSMF DD                                       |  |
| DISP=SHR,DCB=BUFNO=3,DSN=_____ |  |                                                     |  |
|                                |  | // DD                                               |  |
| DISP=SHR,DCB=BUFNO=3,DSN=_____ |  |                                                     |  |
|                                |  |                                                     |  |
|                                |  |                                                     |  |
| +-----+                        |  |                                                     |  |

Figure 7-5. INPUTRDR JCL Definition Worksheet

### 7.3.2.2 INPUTSNT PARS Member JCL Definition

The INPUTSNT member of prefix.MICS.PARMS contains the DD statements to specify the input data for the CA MICS Network Analyzer. The //INPUTSMF DD and, optionally, the //SMFDRCTR DD statements are used by the DAY056 step of the DAILY job.

The INPUTSNT member contains the input SMF data sets when ANY of the following JCLDEF options is used:

- o DAYSMF OFF is specified
- o SMFDRCTR/SMFDIRECTOR SNT is specified
- o DAYSMF EXCLUDE SNT is specified

A //INPUTSMF DD statement is required for each SMF data source.

A //SMFDRCTR DD statement is only required when CA SMF Director split indices are used.

A worksheet for preparing the INPUTSNT member is provided below in Figure 7-6.

If you change the contents of the INPUTSNT member, you must regenerate the CA MICS DAILY job using either JCLGENU or JCLGEND in prefix.MICS.CNTL.

This product processes SMF data from CA NetSpy, NPM Network, NPM Session, NetView Session Monitor/NLDM, NetView Hardware Monitor/NPDA, CA NetMaster NTS, CA NetMaster NEWS, and TCP/IP and the data from the VM versions of CA NetSpy and NPM. The INPUTSNT member can contain JCL definitions for SMF input if you do not specify SMFRECORDING SNT in prefix.MICS.PARMS(JCLDEF). If SMFRECORDING SNT is specified in JCLDEF, it must be defined in the input JCL in the INPUTRDR member in prefix.MICS.PARMS.

Note: If your site has CA SMF Director installed, you can use it to extract specific SMF record types and subtypes at SMF dump time. For more details on this product feature, see section 6.10, CA MICS and CA SMF Director Interface, of this guide.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>+-----+   INSTALLATION PREPARATION WORKSHEET:  INPUTSNT JCL Definitions     PARS Library Member is INPUTSNT                                 +-----+    This definition is required to specify the DD statement for data     that will be read by the DAILY CA MICS job.                                                                                                //@                                                                  //@ WARNING: ALWAYS MAKE CHANGES IN PARS(INPUTSNT) AND NOT        //@                &amp;CNTL(DAILY) .                                   //@                CHANGES MADE TO &amp;CNTL(DAILY)                   //@                WILL BE GONE WHEN DAILY REGENERATED BY JCLGEN.     //@                                                                  //INPUTSMF DD DISP=SHR,DCB=BUFNO=5,DSN=_____                    //                DD DISP=SHR,DCB=BUFNO=5,DSN=_____              //@                                                                  //SMFDRCTR DD DISP=SHR,DCB=BUFNO=5,DSN=_____                     //                DD DISP=SHR,DCB=BUFNO=5,DSN=_____                                                                                   +-----+</pre> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Figure 7-6. INPUTSNT JCL Definition Worksheet

### 7.3.3 JCL Option Definitions (JCLDEF)

There are a few required parameters and many optional ones, which you specify in `prefix.MICS.PARMS(JCLDEF)` to guide the JCLGEN process as it generates CLISTs and jobs tailored for your processing environment. This member contains one statement for each option defined.

All CA MICS Network Analyzer Option input sources (NPM Network, NPM Session, NetView Session Monitor/NLDM, NetView Hardware Monitor/NPDA, CA NetMaster NTS, CA NetMaster NEWS, CA NetSpy, and TCP/IP) are read from SMF history files. If any of these sources or the VM version of CA NetSpy or NPM is used as input to the CA MICS Network Analyzer Option, the `SMFRECORDING` statement in `prefix.MICS.PARMS(JCLDEF)` must be updated during installation with the product identifier SNT. JCLDEF is described in detail in the PIOM, Section 2.3.3.2.1.1.

The `SMFRECORDING` statement is used by the JCLGEN process to build the DAILY job. If more than one CA MICS product that takes input from SMF is specified on the `COMPONENTS` statement (described in Section 2.3.3.2.1.1 in the PIOM), then a job step named `DAYSMT` is generated as the first step of the DAILY job. `DAYSMT` splits the SMF input file (defined by `prefix.MICS.PARMS(INPUTSMF)`) into multiple work files, one for each CA MICS product that takes its input from SMF. The DDname of `INPUTSMF` is used to address the work file in DAILY job steps for products that input such work files.

If there is only one CA MICS product using SMF input, JCLGEN does not create a `DAYSMT` step to split apart the input SMF File. Rather, the SMF File defined in `prefix.MICS.PARMS(INPUTSMF)` goes directly into the DAILY job step for that one product (for example, into `DAY056` for CA MICS Network). The `INPUTSMF` ddname is defined in `prefix.MICS.PARMS` to improve performance in this special case.

### 7.3.4 Network Identifier Exit (SNTNIDRT)

This section explains how to code a network identifier exit for the CA MICS Network Analyzer Option.

The network identifier is an eight-character variable, NETWRKID, which is the highest (most significant) sequence/summary variable in each CA MICS Network Analyzer file. Data from NPM and CA NetSpy network session accounting and network gateway accounting supply values for NETWRKID, so you do not need to code the SNTNIDRT exit for these data sources.

The other data sources supported by the Analyzer do not supply a value for this variable. You must code a unique one to eight-character network identifier for data from each network processed by CA MICS.

If NPM is a data source, there are two fields that may help you to decide the proper value for NETWRKID. Data elements PLUNETID and SLUNETID may contain the PLU and SLU network IDs, respectively. See the Data Dictionary entries for these elements to determine if they may be of value to you. The sample exit provided in Figure 7-7 shows a possible method for deriving NETWRKID from PLUNETID.

The network identifier coded here appears in several places in the CA MICS Network Analyzer:

- o As the highest qualifier in each CA MICS file
- o In the CA MICS Tabular Reports and Graphic Inquiry Reports
- o In SNTOPS - previously described in this chapter

The Network Identifier Exit is a user-written SAS routine that is invoked for each input record processed. You are responsible for testing the accuracy of the routine. A sample network identifier exit routine is provided in prefix.MICS.PARMS(SNTNIDRT). Figure 7-7 shows the worksheet for structuring this routine.

It is important to remember that this routine is invoked before the SMF System Identifier (SYSID) variable has been established. Therefore, if you want to set NETWRKID using the SYSID, you must use the original system identifier, ORGSYSID, as recorded in the data.

+-----+

Chapter 7: PARAMETERS 1191

### 7.3.5 Link TP Circuit ID Exit (SNTCIDRT)

This section explains how to code the teleprocessing (TP) Circuit ID for those CA MICS Network Analyzer files containing data with LINK name as a major sequence/summary variable. This information permits people responsible for hardware maintenance to quickly identify the TP Circuit ID associated with a failing link, thus reducing problem reporting and hardware outage time.

The SNT Link TP Circuit ID Exit is a user-written routine that is invoked for the following Analyzer files:

- o NCP Link (SNTNCL) File
- o NPM Link Activity (SNTNPL) File
- o NLDM Link Activity (NVSNLL) File

The exit is invoked prior to writing observations to these files. Just before calling this user exit, CA MICS sets the variable FILEID equal to NCL, NPL, or NLL so that the exit can determine the source of the link data in the exit code before assigning a value to the Link TP Circuit Identifier (LNKTPCID).

LNKTPCID is a 14-character variable which is initialized from link name and other variables in each of these files. The variables which may be important in setting LNKTPCID in each file are:

- o SNTNCL File
  - . NCPNAME - Network Ctl Program Name
  - . NETNAME - Resource Network Name  
(always the Link Name in this file)
  - . NETWRKID - Network Identifier
  - . SYSID - System Identifier
- o SNTNPL File
  - . NETWRKID - Network Identifier
  - . PLUSA - Primary Logical Unit Subarea Name
  - . SLULINK - Boundary Link (Line) Name
  - . SYSID - System Identifier



## o NVSNLL File

- . NETWRKID - Network Identifier
- . PLUSAPU - Primary Logical Unit Subarea Physical Unit
- . SLULINK - Boundary Link (Line) Name
- . SYSID - System Identifier

The Link TP Circuit ID exit routine is written in SAS code. The testing and accuracy of the exit routine is your responsibility. A sample exit is provided in prefix.MICS.PARMS(SNTCIDRT). The worksheet for structuring this exit routine is shown in Figure 7-8.

```

+-----+
| INSTALLATION PREPARATION WORKSHEET: SNA Network Link TP Circuit ID Exit |
| Routine |
| PARMs Library Member is SNTCIDRT |
| Reference Section: 7.3.5, CA MICS Network Analyzer Guide |
+-----+
|
| /* ----- */
| /* THIS ROUTINE IS USED TO SET THE VALUE OF LNKTPCID. */
| /* THIS ROUTINE IS %INCLUDED JUST PRIOR TO WRITING EACH LINK RELATED */
| /* FILE. */
| /*
| /* FOR EXAMPLE:
| /*
| /* IF NETWRKID = 'DCA3033A' THEN DO;
| /*
| /* IF FILEID = 'NCL' OR FILEID = 'NPL' THEN DO;
| /*
| /* IF NETNAME='L253105' THEN LNKTPCID='TP-471-0012-03';
| /* ELSE IF NETNAME='L253106' THEN LNKTPCID='TP-471-0022-03';
| /* END;
| /*
| /* ELSE IF FILEID = 'NLL' THEN DO;
| /*
| /* IF SLULINK='L253105' THEN LNKTPCID='NY-ATL TG';
| /* ELSE IF SLULINK='L253106' THEN LNKTPCID='NY-CHI TG';
| /*
| /* END;
| /* END;
|

```



### 7.3.6 Network Service Group Definition (NETGROUP)

The CA MICS Network Analyzer supports the data element NETGROUP in each of the six files available for accounting:

- o NCP Network Accounting (SNTNAC) File
- o CA NetSpy Terminal (SNTNSS) File
- o NPM User Activity (SNTPSU) File
- o NLDM Session Accounting (NVSNSA) File
- o NLDM Session Connectivity (NVSNSC) File
- o NLDM Response Time (NVSRTM) File

NETGROUP is used to classify a network session according to its service requirements or its configuration characteristics. The classifications permit differential billing based on service requirements or configuration.

For example, an enterprise may want to charge a premium for sessions that receive a high transmission priority. Sessions with a transmission priority greater than 0 could be charged at the rate of 125% of the normal charge for character traffic. All other sessions would be charged at the standard billable rate (that is, 100%).

Defining network service groups is a two-step process.

First, each network group is identified by a network group number (an identifying number in the range 1-256), a service factor (a value that identifies the rate at which session charges will be assessed), and a description. This information is recorded in prefix.MICS.PARMS(NETGROUP).

Then, a routine is coded to set NETGROUP in the appropriate files so it can be used for network accounting. This routine, called NETGPRT (also a member of prefix.MICS.PARMS), is discussed in Section 7.3.7 of this guide.

NETGROUP is a numeric variable whose value, by CA MICS convention, must be an integer from 1 to 256. The actual value of NETGROUP is not used in any computations or additional processes. It is simply a retained value that is associated with a specific service factor.

You can use the worksheet provided in Figure 7-9 to define NETGROUP. Once the worksheet is complete, transfer the information to prefix.MICS.PARMS(NETGROUP). The rules for completing the worksheet are as follows:

- o All fields, except the description field, are required for each statement.
- o An asterisk (\*) in the first column indicates that the entire statement is a comment.
- o Blank lines are ignored.
- o The format of a statement is freeform, but positional. The form for each statement follows:

GROUP           = Service-factor description

NETGROUP-     = An integer from 1 to 256  
NUMBER

SERVICE-       = Any valid number, with or without  
FACTOR           fractional value

DESCRIPTION = An optional description of the network  
              service group

### Examples

-----

Establishing network groups results from the decision to differentially charge for network resources based on expected service or configuration parameters. You may find the examples below useful in your decision-making process.

### CLASSIFICATION BY CONFIGURATION

Some network users require specialized facilities to ensure high speed transmission, extended availability through redundant hardware, extremely low error rates, or quick response time. Installing high speed links and transmission groups, assigning high transmission priority to specific classes of work (higher priority for interactive rather than batch transmissions), or providing for redundant communication lines are examples of ways in which high priority users may be provided with better service on a network. As a direct result of the additional cost of these facilities or in recognition of the improved service they afford, the enterprise may want to charge a premium for this type of service.

The CA MICS Network Analyzer provides data that can be used to distinguish configuration and service differences, such as link name (SLULINK), controller name (SLUPU), virtual route

number (for example, NSCVRTE), transmission priority (for example, NSCTRPTY), or explicit route (for example, NSCEXRTE).

#### CLASSIFICATION BY LOCATION

An enterprise may want to break the assignment of NETGROUP numbers into blocks, assigning a block of numbers to specific networks. The CA MICS Network Analyzer supports the data element NETWRKID, a user-defined data element you can use to identify individual networks.

#### CLASSIFICATION BY PERFORMANCE CLASS

CA MICS Network Analyzer supports the NetView concept of performance class as the data element PERFCLSS in the NVSRTE, NVSRM, NVNSA, and NVNSC files. The CA NetMaster RTM class is equivalent to the NetView performance class. In this guide, RTM class is referred to as performance class.

Performance classes are defined by each site when NetView or CA NetMaster is installed. PERFCLSS is generally used for classifying or grouping users for reporting response time so that response objectives and distribution thresholds are the same for users who perform similar functions and the response times recorded by the Response Time Monitor may be easily evaluated for each group of users defined to be within the same PERFCLSS.

PERFCLSS may be adapted for use in differential billing so that the charges for one group of users are adjusted to 75 percent of the standard charge assessed for data traffic and connect time to all other users. In this case, a service factor of .75 would be associated with the particular PERFCLSS.

A sample NETGROUP member is shown below:

```
* SAMPLE NETGROUP MEMBER
GROUP 1 1.00 'DEFAULT SERVICE GROUP/FACTOR'
GROUP 2 1.50 'FIBER OPTIC LINKS'
GROUP 3 1.33 'T1 LINKS'
```

In this example, the default network service group is 1, and its corresponding service factor is 1.00. User sessions that fall into this category are charged at the standard

rate for network services. Group 2 is assigned for sessions across fiber optic links; these sessions are charged at the rate of 1.5. Sessions using T1 speed links are charged at a 33 percent premium rate.

| INSTALLATION PREPARATION WORKSHEET: Network Group Definitions |                    |                   |             |
|---------------------------------------------------------------|--------------------|-------------------|-------------|
| PARMS Library Member is NETGROUP                              |                    |                   |             |
| Reference Section: 7.3.6, CA MICS Network Analyzer Guide      |                    |                   |             |
|                                                               | NETGROUP<br>NUMBER | SERVICE<br>FACTOR | DESCRIPTION |
| GROUP                                                         | _____              | _____             | ' _____ '   |
| GROUP                                                         | _____              | _____             | ' _____ '   |
| GROUP                                                         | _____              | _____             | ' _____ '   |
| GROUP                                                         | _____              | _____             | ' _____ '   |
| GROUP                                                         | _____              | _____             | ' _____ '   |
| GROUP                                                         | _____              | _____             | ' _____ '   |
| GROUP                                                         | _____              | _____             | ' _____ '   |
| GROUP                                                         | _____              | _____             | ' _____ '   |
| GROUP                                                         | _____              | _____             | ' _____ '   |
| GROUP                                                         | _____              | _____             | ' _____ '   |
| GROUP                                                         | _____              | _____             | ' _____ '   |
| GROUP                                                         | _____              | _____             | ' _____ '   |
| GROUP                                                         | _____              | _____             | ' _____ '   |
| GROUP                                                         | _____              | _____             | ' _____ '   |
| GROUP                                                         | _____              | _____             | ' _____ '   |
| GROUP                                                         | _____              | _____             | ' _____ '   |
| GROUP                                                         | _____              | _____             | ' _____ '   |
| GROUP                                                         | _____              | _____             | ' _____ '   |
| GROUP                                                         | _____              | _____             | ' _____ '   |
| GROUP                                                         | _____              | _____             | ' _____ '   |
| GROUP                                                         | _____              | _____             | ' _____ '   |

|                                                                         |         |
|-------------------------------------------------------------------------|---------|
|                                                                         |         |
| +-----+                                                                 | +-----+ |
| ...5...10...15...20...25...30...35...40...45...50...55...60...65...70.. |         |
| +-----+                                                                 | +-----+ |

Figure 7-9. Network Group Definition Worksheet

### 7.3.7 Network Service Group Exit Routine (NETGPRT)

This section explains how to code an exit to assign values to the Network Service Group Definition (NETGROUP).

NETGROUP affects the SNTPSU File (NPM Session data), the SNTNSS File (CA NetSpy data), the NVSNSA, NVSNSC, and NVSRM Files (NetView Session Monitor or CA NetMaster NTS data), and the SNTNAC File (CA NetSpy or NPM network session accounting or network gateway accounting data). These definitions occur at the data base unit level (not at the complex level) and must be recoded or copied if the CA MICS Network Analyzer is installed in more than one data base unit.

The Network Service Group Exit Routine in prefix.MICS.PARMS(NETGPRT) is a user-written routine that is invoked for each input record processed. The routine contains valid SAS code which typically interrogates one or more data elements to determine a value for NETGROUP. See Section 7.3.6 for more information on determining the value of NETGROUP.

Figure 7-10 shows a worksheet you can use to code this exit routine. Below is a sample exit routine.

```
/* */
/* SAMPLE NETWORK SERVICE GROUP EXIT ROUTINE */
/* DO NOT EVER CODE A SAS RETURN STATEMENT */
/* */
/* DEFAULT GROUP FOR RATE OF 1.00 */
/* */
NETGROUP=1;
* FIBER OPTIC LINKS BEGIN WITH 'L100', RATE OF 1.50;
IF FILEID='NVSNSC' AND SLULINK='L100' THEN NETGROUP=2;
* T1 LINKS BEGIN WITH 'L200', RATE OF 1.33;
IF FILEID='NVSNSC' AND SLULINK='L200' THEN NETGROUP=3;
IF FILEID='SNTNSS' AND NSSAVTTM LT 3 THEN NETGROUP=2;
```

In this example, the default service charge of 1.00 is used for sessions across standard terrestrial links. NETGROUP is set to 1 for these sessions. For fiber optic links, NETGROUP is set to 2, which is associated with a service rate of 1.5. For T1 links, NETGROUP is set to 3 and the service rate is 1.33. Also, according to the service level agreement that has been established at this site, if the user's average total response time, as measured by CA NetSpy, is less than three seconds, the user is to pay a premium and is assigned to NETGROUP 2.



[illegible]

Figure 7-10. Network Service Group Routine Definition Worksheet

### 7.3.8 Network Application Table (NETAPPL)

The Network Application Table is used to identify applications that are part of application-to-application (APPL-APPL) sessions.

NETAPPL affects the SNTPSU file from the NPM Session data source, the NVSNsc File from either the NetView Session Monitor/NLDM or CA NetMaster NTS data source, and the SNTNAC file from either the CA NetSpy or NPM network session accounting or network gateway accounting data sources.

The format of this table, NETAPPL, is described below. To determine whether or not a given session is an APPL-APPL session, the code compares the secondary logical unit (SLU) name against entries in the NETAPPL table. A match indicates that the logical unit to logical unit (LU-LU) session is an APPL-APPL session, and the local device flag is set to A.

The local device flag is used in conjunction with CA MICS Accounting and Chargeback to differentially charge for local, remote, or APPL-APPL sessions. Section 7.3.6 discusses differential billing using this flag.

Use the worksheet provided in Figure 7-11 to define NETAPPL. Once the worksheet is complete, transfer the information to prefix.MICS.PARMS(NETAPPL). The rules for completing the worksheet are as follows:

- o Each statement may contain a single application identifier. All other fields are considered comments.
- o Comments statements are permitted. An asterisk (\*) in the first column indicates that the entire statement is a comment.
- o Blank lines are ignored.
- o The application name is the same as the one defined on the VTAM APPL statement.

A sample NETAPPL member is shown below:

```
* SAMPLE SNA NETWORK APPLICATION TABLE MEMBER
TSO
CICSTEST
CICSPROD
```

[illegible]

Figure 7-11. SNA Network Application Table

### 7.3.9 PLU Identification Routine (SNTPLURT)

This section explains how to code the Primary Logical Unit (PLU) Identification Routine (SNTPLURT) in prefix.MICS.PARMS.

The SNTPLURT routine is not necessary for data collected by the CA NetSpy NCP interface (except for network session accounting/network gateway accounting data). Moreover, the routine should not be necessary for data collected by the CA NetSpy VTAM interface, as long as you have correctly specified the ALIAS parameter in the CA NetSpy initialization parameters. See the CA NetSpy documentation for additional information.

#### Why and When You Need to Code SNTPLURT

-----

Some VTAM applications, such as TSO and TAF (Terminal Access Facility, which runs under NetView or NCCF), have multiple application (APPL) statements defined to VTAM. This results in multiple names for a single application in NetView Session Monitor, CA NetMaster NTS, and NPM session data, causing two special problems for data in the CA MICS Network Analyzer files.

The first problem applies to NetView, CA NetMaster, NPM session, and NPM or CA NetSpy network session accounting/network gateway accounting data for any application with multiple APPL statements defined.

If an application has multiple APPL statements defined, the CA MICS element Primary Logical Unit (PLU) contains different values for different sessions with this application. This can greatly increase the size of files that have PLU as a sequence/summary element. NPM and its session data collection function, if properly tailored, circumvent this problem (discussed below); which NetView and CA NetMaster do not. The affected files are SNTPSY, SNTPSU, SNTNPL, SNTNAC, NVSLSY, NVSVBF, NVNSA, NVNSC, NVSRTE, and NVSRM.

The second problem is unique to NetView accounting and availability data and CA NetMaster accounting data for TSO sessions.

Two sessions are recorded by NetView and CA NetMaster for every TSO user session: one for the initial session with TCAS and one for the session with a TSO address space. This number is carried in the CA MICS element Number of Sessions (NSCNMSES). Although NSCNMSES is technically accurate, you

may find it more useful for accounting purposes to think of it as only one session.

You can code the CA MICS Network Analyzer routine SNTPLURT in prefix.MICS.PARMS to convert the multiple PLU values to a single PLU name for the application in NetView, CA NetMaster, CA NetSpy or NPM network session accounting data, and, if required, in NPM session data. SNTPLURT also increments NSCNMSES by one only for each TSO user session.

As indicated earlier, NPM session data collection eliminates the problem of incurring multiple values for the PLU element for applications that have multiple application statements defined. See the parameters SYN, SYNCOUNT, and SYNMASK in the APPL initialization statement in the NPM documentation.

#### Coding the Exit

-----

SNTPLURT is invoked for the following NPM files if you code the SAS statement IF COMPT= 'SNT NPM' THEN DO; in the routine:

- o NPM User Activity (SNTPSU) File
- o NPM System Activity (SNTPSY) File
- o NPM Link Activity (SNTNPL) File
- o NCP Network Accounting (SNTNAC) File

SNTPLURT is invoked for the following NLDM files (which may contain NetView Session Monitor/NLDM or CA NetMaster NTS data) if you code the SAS statement IF COMPT= 'SNT NLDM' THEN DO; in the routine:

- o NLDM System Activity (NVSLSY) File
- o NLDM Link Activity (NVSNLL) File
- o NLDM Session Accounting (NVSNSA) File
- o NLDM Session Connectivity (NVSNSC) File
- o NLDM Response Time (NVSRTM) File
- o NLDM Route (NVS RTE) File
- o NLDM VTAM BIND Failure (NVS VBF) File

SNTPLURT is written in the SAS language. The testing and accuracy of the process is the responsibility of the user. However, the CA MICS Network Analyzer provides a sample SNTPLURT exit routine and certain program aids to help verify the accuracy of your modifications to the routine. The worksheet for structuring the SNTPLURT exit routine is shown in Figure 7-12.

To code the SNTPLURT exit for an application, review the major node definitions in SYS1.VTAMLST that contain the APPL statements for that application. See the IBM VTAM documentation for information on defining applications to VTAM.

Below are examples of how APPL statements could appear for two TS0 systems on two different hosts, and of two alternative examples for coding SNTPLURT:

```

** Note: The first APPL statement below is for TCAS **
TS010 APPL AUTH=AUTH(NOACQ=PASS,NVPACE,TS0,NOP0), X
 EAS=1,ACBNAME=TS0
** Note: The additional APPL statements below are for **
** as many users as will be logged on to TS010 at one time.**
TS01001 APPL AUTH=AUTH(NOACQ=PASS,NVPACE,TS0,NOP0), X
 EAS=1,ACBNAME=TS00001
TS01002 APPL AUTH=AUTH(NOACQ=PASS,NVPACE,TS0,NOP0), X
 EAS=1,ACBNAME=TS00002
- - -
- - -
- - -
TS01060 APPL AUTH=AUTH(NOACQ=PASS,NVPACE,TS0,NOP0), X
 EAS=1,ACBNAME=TS00060

** Note: The first APPL statement below is for TCAS **
TS015 APPL AUTH=AUTH(NOACQ=PASS,NVPACE,TS0,NOP0), X
 EAS=1,ACBNAME=TS0
** Note: The additional APPL statements below are for **
** as many users as will be logged on to TS015 at one time.**
TS01501 APPL AUTH=AUTH(NOACQ=PASS,NVPACE,TS0,NOP0), X
 EAS=1,ACBNAME=TS00001
TS01502 APPL AUTH=AUTH(NOACQ=PASS,NVPACE,TS0,NOP0), X
 EAS=1,ACBNAME=TS00002
- - -
- - -
- - -
TS01540 APPL AUTH=AUTH(NOACQ=PASS,NVPACE,TS0,NOP0), X
 EAS=1,ACBNAME=TS00040

```

In the first example below, the SNTPLURT routine does the following:

- o Sets the value of PLU to TS010 for all synonym values of TS010 (that is, TS01001 thru TS01060).
- o Sets the value of PLU to TS015 for all synonym values of TS015 (that is, TS01501 thru TS01540).

- o Prevents the NVNSA file element, Number of Sessions (NSCNMSES) from being incremented for TCAS sessions using TS010 and TS015, by setting the Number of Sessions counter to zero for all TCAS sessions in the DETAIL timespan.

```

* THIS ROUTINE IS USED TO SET THE VALUE OF PLU FOR
* APPLICATIONS, SUCH AS TS0, THAT HAVE SYNONYMS DEFINED.
*
*
* EXAMPLE 1:
;
IF COMPT='SNT NPMS' THEN DO; /* NPM SESSION DATA*/
 IF PLU='TS010' THEN PLU='TS010 ';
 IF PLU='TS015' THEN PLU='TS015 ';
END;
/* NETVIEW SESSION MONITOR OR CA NetMaster NTS DATA*/
IF COMPT='SNT NLDM' THEN DO;
 IF PLU='TS010' THEN NSCNMSES=0;
 ELSE IF PLU='TS010' THEN PLU='TS010 ';
 IF PLU='TS015' THEN NSCNMSES=0;
 ELSE IF PLU='TS015' THEN PLU='TS015 ';

END;

```

The SNTPLURT routine in the second example is similar to the routine shown in the first example in that NSCNMSES is not incremented for TCAS sessions in TS010 and TS015. However, instead of setting NSCNMSES to zero for TCAS sessions, the routine deletes the observations for the TCAS session altogether.

```

* EXAMPLE 2:
;
IF COMPT='SNT NPMS' THEN DO; /* NPM SESSION DATA*/
 IF PLU='TS010' THEN PLU='TS010 ';
 IF PLU='TS015' THEN PLU='TS015 ';
END;
/* NETVIEW SESSION MONITOR OR CA NetMaster NTS DATA */
IF COMPT='SNT NLDM' THEN DO;
 IF PLU='TS010' THEN DO;
 EXITS=BLANKS;
 GOTO OPTN_DEL;
 END;
 IF PLU='TS015' THEN DO;
 EXITS=BLANKS;
 GOTO OPTN_DEL;
 END;
END;

```

|         |                                                                         |
|---------|-------------------------------------------------------------------------|
| +-----+ |                                                                         |
|         | INSTALLATION PREPARATION WORKSHEET: PLU Identifier Exit Routine         |
|         | Definition                                                              |
|         | PARMS Library Member is SNTPLURT                                        |
|         | Reference Section: 7.3.9, CA MICS Network Analyzer Guide                |
| +-----+ |                                                                         |
|         |                                                                         |
|         | /* ----- */                                                             |
|         | /* THIS ROUTINE IS USED TO SET THE VALUE OF PLU FOR APPLICATIONS, */    |
|         | /* SUCH AS TSO, THAT HAVE SYNONYMS DEFINED. */                          |
|         | /* */                                                                   |
|         | /* */                                                                   |
|         | /* FOR EXAMPLE: */                                                      |
|         | /* */                                                                   |
|         | /* IF COMPT='SNT NPMS' THEN DO; /* NPM SESSION DATA*/                   |
|         | /* IF PLU='TS010' THEN PLU='TS010 ';                                    |
|         | /* IF PLU='TS015' THEN PLU='TS015 ';                                    |
|         | /* END; */                                                              |
|         | /* IF COMPT='SNT NLDM' THEN DO; /* NETVIEW SESSION MONITOR DATA*/       |
|         | /* IF PLU='TS010' THEN NSCNMSES=0; */                                   |
|         | /* ELSE IF PLU='TS010' THEN PLU='TS010 ';                               |
|         | /* IF PLU='TS015' THEN NSCNMSES=0; */                                   |
|         | /* ELSE IF PLU='TS015' THEN PLU='TS015 ';                               |
|         | /* */                                                                   |
|         | /* END; */                                                              |
|         | /* */                                                                   |
|         |                                                                         |
|         |                                                                         |
|         |                                                                         |
|         |                                                                         |
|         |                                                                         |
|         |                                                                         |
|         |                                                                         |
| +-----+ |                                                                         |
|         | ...5...10...15...20...25...30...35...40...45...50...55...60...65...70.. |
| +-----+ |                                                                         |

Figure 7-12. PLU Identifier Exit Routine Definition Worksheet



### 7.3.10 Database Space Modeling (DBMODEL)

This section describes the information required to define the Analyzer to the Database Space Modeling Facility. Specifically, the user must provide values for the cycle (data retention) definitions. The special considerations for defining the FILE input statements to the Database Space Modeling facility are discussed.

Section 2.3.4 of the PIOM, Database Space Modeling Facility, explains how these values are used in estimating the DASD requirements of the database, and how the user can input these values to the modeling facility.

This section covers the following topics:

- 1 - Data Retention Specifications (FILE Statements)

### 7.3.10.1 Data Retention Specifications (FILE Statements)

This section describes data retention definitions required for the CA MICS Network Analyzer, discusses how to determine the number of data cycles required, and provides instructions for completing the FILE statements in the `prefix.MICS.PARMS(DBMODEL)`.

Figure 7-13 provides a worksheet to define the different retention limits for the online and archive database files. The numbers shown on the worksheet reflect the default retention values in `prefix.MICS.PARMS(DBMODEL)`.

Use the worksheet to define your retention specifications, which in turn will allow you to determine the appropriate values for the modeling process. The worksheet below contains only the Network Analyzer values.

The worksheet is organized by information area. Each file in the area is listed by name. For each file, a line is formatted to allow six definitions in the online database and two in the archive database:

- o The online database files quantify the number of cycles of data that is maintained in the DETAIL, DAYS, WEEKS, MONTHS, and YEARS timespans and the TABLES data area.
- o The two definitions for the archive database files quantify the number of cycles of data to be retained, up to the cutoff limit defined. The archive definitions have no impact on the size of the database and can be specified whethert the weekly and/or monthly archive history files have actually been activated (see Section 2.3.3, CA MICS JCL Planning and Parameters, of the PIOM).

The worksheet formats provide an underscored area for the user's definition, followed by the recommended value, shown within parentheses. If the underscored area contains a value of 00, the file is not supported for the indicated timespan. To add support, perform database tailoring as described in Section 6.2, Tailoring the Database, of the System Modification Guide (SMG).

When specifying a retention limit, remember that the number may never be zero if the file has been defined to be active in the timespan.

The FILE statements shown below specify the default online

and archive history retention limits for each of these files.

| +-----+<br>  INSTALLATION PREPARATION WORKSHEET: Database Data Retention Definitions  <br>  PARMS Library Member is DBMODEL  <br>+-----+ |         |         |         |         |       |         |                                 |          |       |
|------------------------------------------------------------------------------------------------------------------------------------------|---------|---------|---------|---------|-------|---------|---------------------------------|----------|-------|
| +-----+ Online Database Retention +-----+                                                                                                |         |         |         |         |       |         | +-----+ Archive Cut-Off +-----+ |          |       |
| File                                                                                                                                     | DETAIL  | DAYS    | WEEKS   | MONTHS  | YEARS | TABLES  | WEEKS                           | MONTHS   |       |
| Name                                                                                                                                     |         |         |         |         |       |         |                                 |          |       |
| +-----+                                                                                                                                  |         |         |         |         |       |         |                                 |          |       |
| SNTNCL                                                                                                                                   | __ (03) | __ (07) | __ (03) | __ (03) | 0 (0) | 00 (00) | __ (053)                        | __ (024) |       |
| SNTCAF                                                                                                                                   | 00 (00) | __ (10) | __ (03) | __ (03) | 0 (0) | 00 (00) | __ (053)                        | __ (024) |       |
| SNTNAF                                                                                                                                   | __ (01) | __ (10) | __ (09) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (024) |       |
| SNTNIN                                                                                                                                   | __ (33) | __ (00) | __ (00) | __ (02) | 0 (0) | 00 (00) | __ (000)                        | __ (024) |       |
| SNTNEF                                                                                                                                   | __ (07) | __ (07) | __ (09) | __ (06) | 2 (2) | 00 (00) | __ (053)                        | __ (024) |       |
| SNTNSF                                                                                                                                   | __ (07) | __ (07) | __ (09) | __ (06) | 2 (2) | 00 (00) | __ (053)                        | __ (024) |       |
| SNTLNF                                                                                                                                   | __ (01) | __ (07) | __ (04) | __ (11) | 0 (0) | 00 (00) | __ (053)                        | __ (024) |       |
| SNTGAF                                                                                                                                   | __ (01) | __ (07) | __ (04) | __ (11) | 0 (0) | 00 (00) | __ (053)                        | __ (024) |       |
| SNTPSU                                                                                                                                   | __ (01) | __ (03) | __ (03) | __ (00) | 0 (0) | 00 (00) | __ (053)                        | __ (000) |       |
| SNTPSY                                                                                                                                   | 00 (00) | __ (07) | __ (09) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (024) |       |
| SNTNPL                                                                                                                                   | 00 (00) | __ (07) | __ (09) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (024) |       |
| SNTNLP                                                                                                                                   | __ (01) | __ (10) | __ (09) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (024) |       |
| SNTNTS                                                                                                                                   | __ (02) | __ (07) | __ (04) | __ (11) | 0 (0) | 00 (00) | __ (053)                        | __ (024) |       |
| SNTNSV                                                                                                                                   | __ (03) | __ (15) | __ (13) | __ (13) | 0 (0) | 00 (00) | __ (053)                        | __ (024) |       |
| SNTNSP                                                                                                                                   | __ (00) | __ (07) | __ (09) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (024) |       |
| SNTNSS                                                                                                                                   | __ (01) | __ (05) | __ (05) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (024) |       |
| SNTNAC                                                                                                                                   | __ (01) | __ (07) | __ (04) | __ (11) | 0 (0) | 00 (00) | __ (053)                        | __ (024) |       |
| SNTNA1                                                                                                                                   | __ (01) | __ (00) | __ (00) | __ (00) | 0 (0) | 00 (00) | __ (000)                        | __ (000) |       |
| SNTNVR                                                                                                                                   | __ (01) | __ (05) | __ (05) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (024) |       |
| NVSLSY                                                                                                                                   | 00 (00) | __ (07) | __ (09) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (025) |       |
| NVSNULL                                                                                                                                  | 00 (00) | __ (07) | __ (09) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (025) |       |
| NVS RTE                                                                                                                                  | __ (01) | __ (05) | __ (05) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (025) |       |
| NVSRTM                                                                                                                                   | __ (01) | __ (05) | __ (05) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (025) |       |
| NVSNSA                                                                                                                                   | __ (01) | __ (05) | __ (05) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (025) |       |
| NVSNSC                                                                                                                                   | __ (01) | __ (05) | __ (00) | __ (00) | 0 (0) | 00 (00) | __ (000)                        | __ (000) |       |
| NVSNS1                                                                                                                                   | __ (01) | __ (00) | __ (00) | __ (00) | 0 (0) | 00 (00) | __ (000)                        | __ (000) |       |
| NVS VBF                                                                                                                                  | __ (07) | __ (07) | __ (09) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (025) |       |
| TCPSTN                                                                                                                                   | __ (07) | __ (07) | __ (09) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (025) |       |
| TCPCTN                                                                                                                                   | __ (07) | __ (07) | __ (09) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (025) |       |
| TCPFSF                                                                                                                                   | __ (07) | __ (07) | __ (09) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (025) |       |
| TCPFCF                                                                                                                                   | __ (07) | __ (07) | __ (09) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (025) |       |
| TCPAPI                                                                                                                                   | __ (07) | __ (07) | __ (09) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (025) |       |
| TCPIPX                                                                                                                                   | __ (07) | __ (07) | __ (09) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (025) |       |
| TCPICX                                                                                                                                   | __ (07) | __ (07) | __ (09) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (025) |       |
| TCP TCI                                                                                                                                  | __ (07) | __ (07) | __ (09) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (025) |       |
| TCPUDI                                                                                                                                   | __ (07) | __ (07) | __ (09) | __ (06) | 0 (0) | 00 (00) | __ (053)                        | __ (025) |       |
| +-----+                                                                                                                                  |         |         |         |         |       |         |                                 |          |       |
|                                                                                                                                          | ...5... | 10...   | 15...   | 20...   | 25... | 30...   | 35...                           | 40...    | 45... |
|                                                                                                                                          | 50...   | 55...   | 60...   | 65...   | 70..  |         |                                 |          |       |
| +-----+                                                                                                                                  |         |         |         |         |       |         |                                 |          |       |

Figure 7-13. Database Data Retention Worksheet

# Chapter 8: MANAGEMENT SUPPORT APPLICATION INTERFACES

---

The CA MICS System encompasses several management support applications that extend the capabilities of CA MICS by processing information that is stored in the database. This chapter describes the interface between the CA MICS Network Analyzer.

This section contains the following topics:

[8.1 CA MICS Accounting and Chargeback Interface](#) (see page 1213)

[8.2 CA MICS Capacity Planner Interface](#) (see page 1220)

## 8.1 CA MICS Accounting and Chargeback Interface

Chargeback for network resources is provided through an interface to CA MICS Accounting and Chargeback. You may use data in CA MICS Network Analyzer files as the basis for network charging for character traffic, connect time, number of sessions, and response events. Special features, as described in Chapter 6 of this guide, permit differential charging based on service factors or configuration parameters.

This section of the chapter briefly discusses why network chargeback is important and how setting rates for network charges may vary depending upon the structural philosophy of the enterprise. It also includes the table of billable elements listing your choices for the network measurements that may be billed using this interface. Finally, there is a section on special considerations that you should evaluate before you make the decision to implement the basic network accounting interface. The following topics are discussed:

- 1 - Chargeback Considerations
- 2 - Billable Elements
- 3 - Network Accounting Considerations

### 8.1.1 Chargeback Considerations

The CA MICS Accounting and Chargeback Option supports the following CA MICS Network Analyzer files for chargeback processing:

- o NCP Network Accounting (SNTNAC) File
- o CA NetSpy Terminal (SNTNSS) File
- o NPM User Activity (SNTPSU) File
- o NLDM Session Accounting (NVSNSA) File
- o NLDM Session Connectivity (NVSNSC) File
- o NLDM Response Time (NVSRTM) File
  
- o NLDM Route (NVS RTE) File

The NCP Network Accounting File can be built from either CA NetSpy network session accounting data/network gateway accounting data or Tivoli NetView Performance Monitor (NPM) network session accounting data/network gateway accounting data. The CA NetSpy Terminal File is built from CA NetSpy's VTAM interface data. The NPM User Activity File is built from Tivoli's NPM Session data. The NLDM files are built using data from either Tivoli's NetView Session Monitor/NLDM or CA NetMaster Network Tracking System (NTS). The Telnet file is built from CA NetSpy TCP/IP interface.

Using these data sources for chargeback extends the capabilities of CA MICS by allowing the cost of the data communications network to be recovered directly rather than being absorbed as an overhead. This section discusses the advantages of using this approach.

From an accounting standpoint, it is always preferable to recover costs based upon direct measurements rather than allocating overhead charges because the factors used to allocate overhead charges are estimates. Direct measurements eliminate guesswork and have the additional benefit of varying immediately when system or environmental changes cause the use of a resource to vary.

Although valuable, you must apply direct measurements only to those resources that are directly measured. In the case of network data, only use of the network transport resource is measured. Significant errors in resource allocation would result from using this data to apportion, for instance, CPU consumption. For example, you could assume that the utilization of all data processing resources is proportional to the amount of data transmitted on the network. Experience would show that many tasks, such as DB2 inquiries, could

consume vast amounts of CPU resources while generating relatively little network traffic, either for the inquiry or the response.

Limiting the use of network data only to the allocation of the costs of the data transmission resources still produces considerable latitude in the types of algorithms implemented. This is because the algorithm must reflect the organization's structural philosophy, which may or may not be reflected in the design of the network. The remainder of this section discusses three chargeback scenarios for networks with identical topologies that are operated by organizations with differing structural philosophies.

#### THE EXAMPLE NETWORK

In the following examples, the network consists of two sites, as shown in Figure 8-1.

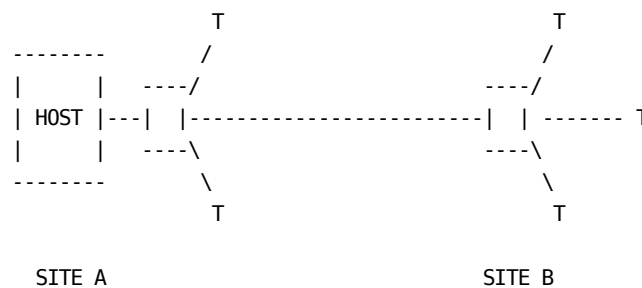


Figure 8-1. Example Network

Site A has the host processing resources and a communications processor (37xx equivalent) while Site B has only a communications processor. Both sites have terminals attached to the network.

#### DATA PROCESSING AS A CENTRALIZED CORPORATE SERVICE

In this case, data processing is viewed by the organization as a tightly controlled, centralized service. Decisions concerning the type of service, level of service, network topology, line speeds, terminals utilized, and so on are made by the central communications staff.

The cost of communications is allocated to end-users based solely upon the volume of data transmitted. The total communications costs are divided by the total traffic load to produce a cost-per-byte factor. This factor is then applied to all traffic. This factor is typically adjusted on an annual basis.

Because the user makes no decisions concerning the line speed, routing of transmissions, or service level of the applications, these factors are not taken into account when setting rates. It is assumed that the design of the network will maximize the cost/performance ratio as defined by the corporate planners.

### DATA TRANSMISSION AS A CENTRALIZED RESOURCE

In this case, data processing is viewed as a resource to be shared equally by all entities within the organization. The corporate communications network provides the connection to this shared resource. Typically, the user is responsible for the costs of the boundary circuits, terminal control units, modems, and local support personnel.

Costs of the corporate network are allocated based on traffic volume and distance from a virtual host processor resource that is located equidistant from all users (despite the fact that the real data center is located at Site A). Charges can also be based on a standard corporate network link speed and can be adjusted for varying link speeds.

### GUEST USERS

In this case, Site B is a paying guest of Site A. Site B, which can be an acquired subsidiary of Site A, gains some advantage from using Site A's processing resources.

Site B bears the total cost of the data transmission to Site A regardless of the distance. Site A does not subsidize Site B's communications costs, as in the previous example, even though Site A can choose, install, and support all of the communication equipment.

Costs are allocated by simply totaling the costs of communication and dividing them by Site B's traffic volume to arrive at a cost-per-byte factor, as in the first example.



#### SUMMARY

In each of these examples, only the actual communications costs are recovered (for example, modems, terminals, control units, links, support personnel, test equipment, and so on). Host processor costs are still recovered based on an application's consumption of host resources.

The differences in algorithms result from the interpretation of what portion of the resources belongs to the corporation as a whole and what portion belongs to the end-user.

### 8.1.2 Billable Elements

CA MICS Network Analyzer files contain specific data elements that may be used for billing through CA MICS Accounting and Chargeback. Chapter 4 in the CA MICS Accounting and Chargeback User Guide lists the charging elements for this component.

### 8.1.3 Network Accounting Considerations

Before you implement basic network accounting using the CA MICS Network Analyzer and CA MICS Accounting and Chargeback, you should review the considerations listed in this section. The following topics are covered:

- 1 - Chargeback Limitations
- 2 - Data Source Operational Considerations
- 3 - Redundant Information Issues

### 8.1.3.1 Chargeback Limitations

The data sources providing data for use in the basic network accounting feature of CA MICS are restricted to identifying session information by primary logical unit (PLU) and secondary logical unit (SLU). In a standard terminal session with an application, PLU corresponds to the name of the application (e.g., TSO, CICSTEST) and SLU corresponds to the terminal identifier. There is no identification of the user (e.g., TSO or CMS USERID) or the account code in the data sources. Therefore, there is an implicit restriction when using CA MICS basic network accounting that charges may be assessed at no more precise level than by terminal within application.

### 8.1.3.2 Data Source Operational Considerations

Chargeback usually requires the measurement and billing of all users of a service. In the case of network chargeback, the implication of this billing approach is that data must be collected for all terminal users of the network(s).

In determining the source for network billing information (NPM, NetView, or NetMaster), you must consider the resources you need to produce the raw information for the chargeback process.

Monitoring a medium to large data network may be more costly in resources (CPU time, virtual storage, volume of data) than you anticipate. Therefore, before you decide on a source, we recommend that you activate the product of your choice and determine its operational impact. Consult the vendor supplying the product to ensure that implementation of the product is optimal and that you have applied all performance-related maintenance.

### 8.1.3.3 Redundant Information Issues

The CA MICS Accounting and Chargeback Option supports the following CA MICS Network Analyzer Option files for chargeback processing:

- o NCP Network Accounting (SNTNAC) File
- o CA NetSpy Terminal (SNTNSS) File
- o NPM User Activity (SNTPSU) File
- o NLDM Session Accounting (NVSNSA) File
- o NLDM Session Connectivity (NVSNSC) File
- o NLDM Response Time (NVSRTM) File

The NCP Network Accounting File is built from network session accounting (NSA) and network gateway accounting (NGA) data from either CA NetSpy or Tivoli NetView Performance Monitor (NPM). The NPM User Activity File is built from NPM Session data. The NLDM files are built using data from either Tivoli NetView Session Monitor/NLDM or CA NetMaster Network Tracking System (NTS). The CA NetSpy Terminal File is built from CA NetSpy's VTAM interface data.

Because there can be overlap between data from these sources, the CA MICS Accounting and Chargeback Option prevents the use of both NPM and NetView Session Monitor/NLDM files concurrently for billing. Should you require the ability to implement chargeback using both NPM and NetView Session Monitor/NLDM or both NPM and CA NetMaster sources, contact Technical Support at <http://ca.com/support>.

CA NetSpy and NPM can collect NSA data on both the secondary (SLU) and primary (PLU) side of a session. To prevent collection of redundant accounting data, collect NSA data on the secondary side of a session only. If your site collects NSA data on both the primary and secondary sides of a session, CA MICS data element NACCOLPT, NCP Collection Point (Primary or Secondary), can help you detect and eliminate redundant NSA data.

Similarly, CA NetSpy and NPM can collect redundant NGA data for sessions that traverse multiple gateway NCPs. To aid in the detection and elimination of this redundant data, collect all NGA data at a single CA NetSpy or NPM collection host. CA NetSpy automatically discards redundant NGA data. It only accepts NGA data for a given session from the first gateway NCP to send it for that session. NPM provides a user exit for detecting and discarding redundant NGA data. See the Tivoli NPM documentation. CA MICS data elements NACANPLU

(Adjacent Network ID SLU Side), NACANSLU (Adjacent Network ID PLU Side), and USESSIDC (Unique Session ID) can also be used to detect and eliminate redundant NGA data.

## 8.2 CA MICS Capacity Planner Interface

CA MICS Capacity Planner support for the CA MICS Network Analyzer is automatically provided for you as long as both products are installed in the same CA MICS complex.

# Chapter 9: PROCESSING

---

Creating and maintaining a large database system such as CA MICS requires closely monitoring its periodic updating processes.

It is vital to the system's effectiveness that the database be updated daily to build the required daily, week-to-date, month-to-date, and year-to-date files accurately. This data collection process for the CA MICS Network Analyzer is vital to the proper operation of this product.

This section contains the following topics:

[9.1 Processing Considerations](#) (see page 1222)

[9.2 DAILY Update Processing Flow](#) (see page 1224)

## 9.1 Processing Considerations

The CA MICS Network Analyzer update process is unique to CA MICS because it involves reading two input files from different DD statements. The DAILY update process reads the INPUTSMF DD statement processing SMF type 28, 37, 39, 118, and 119 records. Then it switches to the INPUTSNT DD statement and processes the NPM Session Statistics Detail records.

### Checkpoint Update

-----

To distinguish the input of CA MICS Network and permit you to invoke the SELECT or FORCE functions for any of the input data sources, an entry is made in the CA MICS checkpoint file, prefix.MICS.CHECKPT.DATA, for each source and unique SYSID. A typical checkpoint file entry after the DAY056 update step would look like this:

```
SYSA SNT NPDA 20AUG05:12:49:29.33 20AUG05:16:17:57.41
SYSA SNT NPMN 20AUG05:10:29:49.41 20AUG05:16:08:29.54
SYSA SNT NLDM 20AUG05:03:00:00.67 20AUG05:08:00:04.88
SYSB SNT NPDA 21AUG05:18:37:06.44 21AUG05:18:44:04.88
SYSC SNT NPMS 21AUG05:06:29:45.00 21AUG05:18:35:46.00
SYSC SNT TCP 10NOV05:08:24:93.00 10NOV05:23:59:99.91
```

The first three entries are for SYSID SYSA and include data from NetView Hardware Monitor/NPDA, Network Performance Monitor Network (NPMN) (network), and NetView Session Monitor/NLDM. The fourth entry is for SYSID SYSB and includes only data from NetView Hardware Monitor/NPDA. The fifth entry is from SYSID SYSC and its input is from NetView Performance Monitor Session (NPMS) data. The last entry is from SYSID SYSC and its input is from IBM TCP/IP Telnet, FTP, and Stack data.

### Select and Force

-----

Should it be necessary to use the SELECT or FORCE option (described in Section 4.3 of the PIOM), ensure that all required data is selected.

### Missing Data

-----

It is possible (even likely in some environments) that there will be days in which there is no data for some of the SYSIDs

from all of the monitors involved. In these cases, the system administrator should ensure that this is intentional and data has not been lost due to software or operational problems. The DAY056 step processes normally if any input data is received for any SYSID defined to this data base unit. See Chapter 10 of this guide for an exit example that you could use to detect a situation in which data is missing for expected SYSIDs and data sources (\_USRIHL exit).

If it is possible to have update runs where there is no data from any SYSID, specify SYSPARM=NODATA on the EXEC statement for the DAY056 step to prevent a USER 300 ABEND.

## 9.2 DAILY Update Processing Flow

This section describes the DAILY processing flow of the CA MICS Network Analyzer Option and the locations of the user exit points. Exits are documented in Chapter 10 of this guide.

The CA MICS Network update process is divided into four distinct processing phases:

- o Process Input Data
- o Database DETAIL/DAYS Timespan Output
- o Database Timespan Update
- o File Aging

### Process Input Data

-----

In this phase, the NPM, CA NetSpy, NetView, NLDM, NPDA, and CA NetMaster data records are read from the INPUTSMF and INPUTSNT DD statements, the input data fields are processed and formatted to create interim SAS records, and the records are written to interim SAS work files.

The following user exits are invoked in this phase:

- o Product Input Exits

- \_USRSEL - File Processing Selection
  - \_USRIHL - Checkpoint File Inspection
  - \_USRSNLW - NLDM Session Data Work File Exit
  - \_USRSNNW - NPM Network Components Work File Exit
  - \_SNTXCON - Configuration Modification Exit

- o Product Output Exits

- Direct exits:

These exits are provided as stub macros in sharedprefix.MICS.SOURCE. You can update these macros to manipulate observations before they are written out.

- \_USRSNCL - NPM/NCP Link File Exit
    - \_USRSCAF - Network Components Activity File Exit
    - \_USRSNAF - NPM/NCP Activity File Exit
    - \_USRSNEF - NPDA Event File Exit



\_USRSNIN - NPM Incident File Exit  
 \_USRSNPL - NPM Link Activity File Exit  
 \_USRSPSY - NPM System (PLU) Activity File Exit  
 \_USRSLSY - NLDL System (PLU) Activity File Exit  
 \_USRSNLL - NLDL Link Activity File Exit  
 \_USRSNLP - NCP Line Processor Activity File Exit  
 \_USRSNSF - NPDA Statistical File Exit  
 \_USRSPSU - NPM User Activity File Exit  
 \_USRSNSV - NLDL Service File Exit  
 \_USRSNSA - NLDL Session Accounting File Exit  
 \_USRSNSC - NLDL Session Connectivity File Exit  
 \_USRSRTE - NLDL Route File Exit  
 \_USRSRTM - NLDL Response Time File Exit  
 \_USRSVBF - NLDL VTAM Bind Failure File Exit  
 \_USRSVBS - VTAM Buffer Data File Exit  
 \_USRSVCS - VTAM CSM Data File Exit  
 \_USRSVGB - VTAM Global Data File Exit  
 \_USRSNSP - CA NetSpy PLU (Application) File Exit  
 \_USRSNSS - CA NetSpy SLU (Terminal) File Exit  
 \_USRSNVR - CA NetSpy Virtual Route Activity File Exit  
 \_USRSNAC - NCP Network Accounting File Exit  
 \_USRSLNF - LAN File Exit  
 \_USRSGAF - Generic Alert File Exit  
 \_USRXCAF - SNTCAF DETAIL Timespan Exit

- Indirect exits:

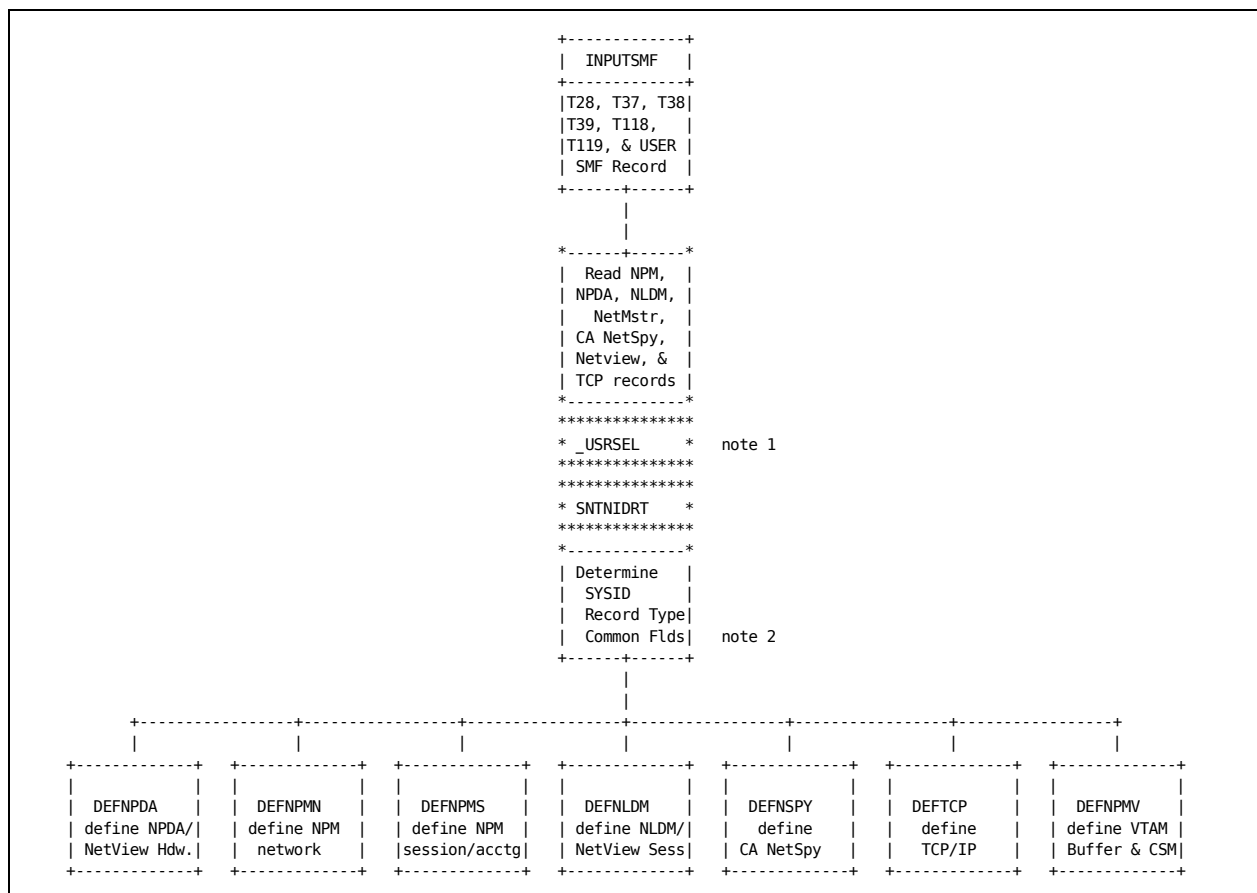
These exits are defined by coding a SAS macro variable to indicate the name of a user source library member. For detailed information on coding exit routines, see Section 3.4 of the System Modification Guide.

USRSNTS - Telnet Server Entry File Exit  
 USRSSTN - Telnet Server File Exit  
 USRSCTN - Telnet Client File Exit  
 USRSFLF - FTP Login Failure File Exit  
 USRSFSF - FTP Server File Exit  
 USRSFCF - FTP Client File Exit  
 USRSAPI - API Calls for Sockets File Exit  
 USRSIPX - IP Statistics File Exit  
 USRSICX - ICMP Statistics File Exit  
 USRSTCI - TCP Statistics File Exit  
 USRSUDI - UDP Statistics File Exit

#### o Product Parameter-Related Exits

SNTACRT - Network Account Code Derivation Exit  
 SNTCIDRT- Link TP Circuit ID Definition Exit  
 SNTNIDRT- Network Identifier Definition Exit

SNTPLURT- PLU (Application) Processing Exit  
 NETGPRT - Network Service Group Definition Exit



Note 1: This exit is entered for all products.

Note 2: Common fields are determined at this point:  
 HOUR, DAY, DAYNAME, WEEK, MONTH, YEAR, ZONE, SYSID

Note: All logic bounded by \*\*\*\*\* indicates a user routine or exit.

Figure 9-1. General Input Process (All Data Sources)

#### Database DETAIL/DAYS Timespan Output

-----

The interim SAS files built in phase 1 are used to create the appropriate files in the CA MICS database's DETAIL or DAYS timespans (whichever is the lowest level timespan for the file).

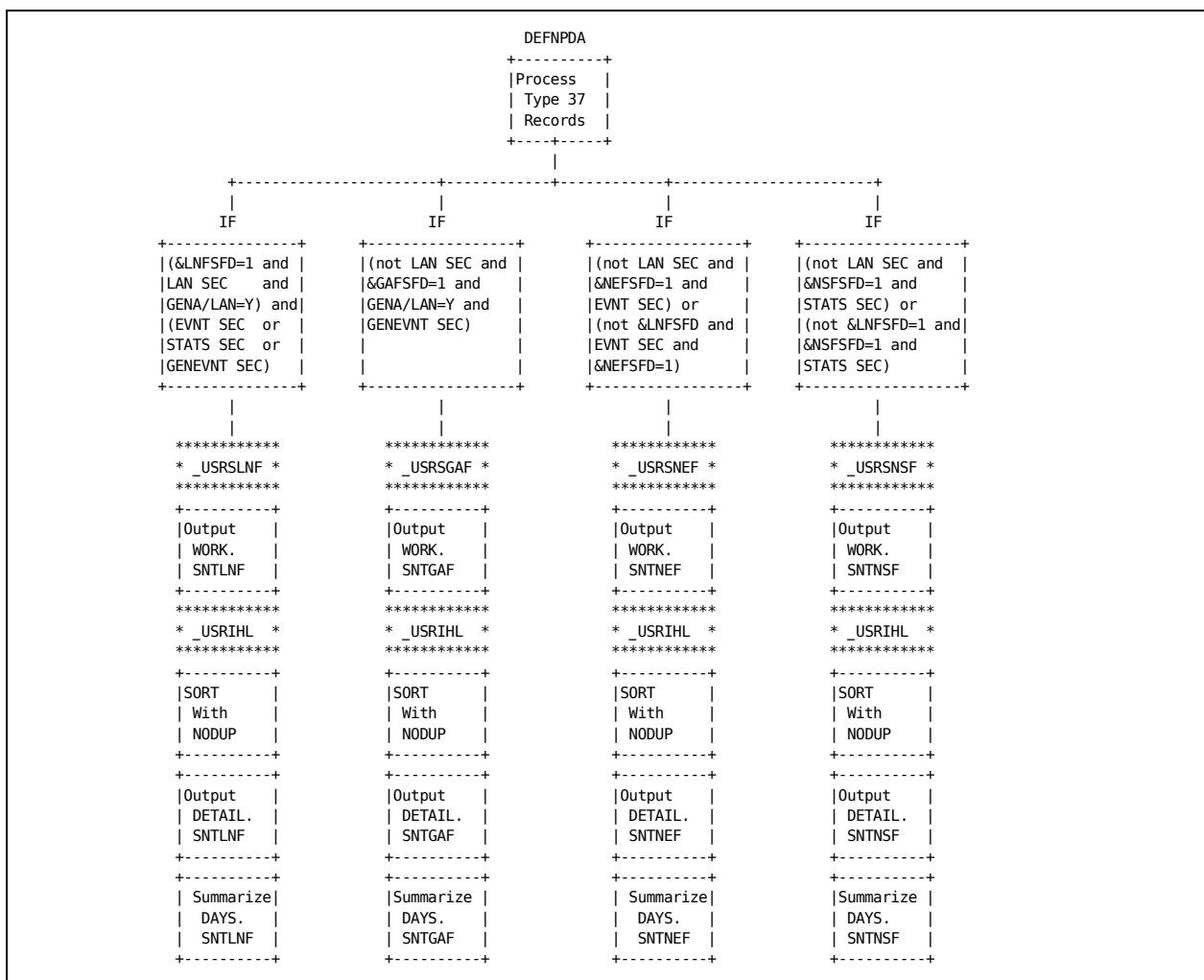
The following user exits are invoked in this phase:

#### o Product Output Exits

- \_USRXCAF - SNTCAF DETAIL Timespan File Exit
- \_USRSCAF - NPM Components Activity File Exit
- \_USRSLSY - NLDM PLU (Application) File Exit
- \_USRSNLL - NLDM Link Activity File Exit
- \_USRSNPL - NPM Link Activity File Exit
- \_USRSPSY - NPM System (PLU) Activity File Exit

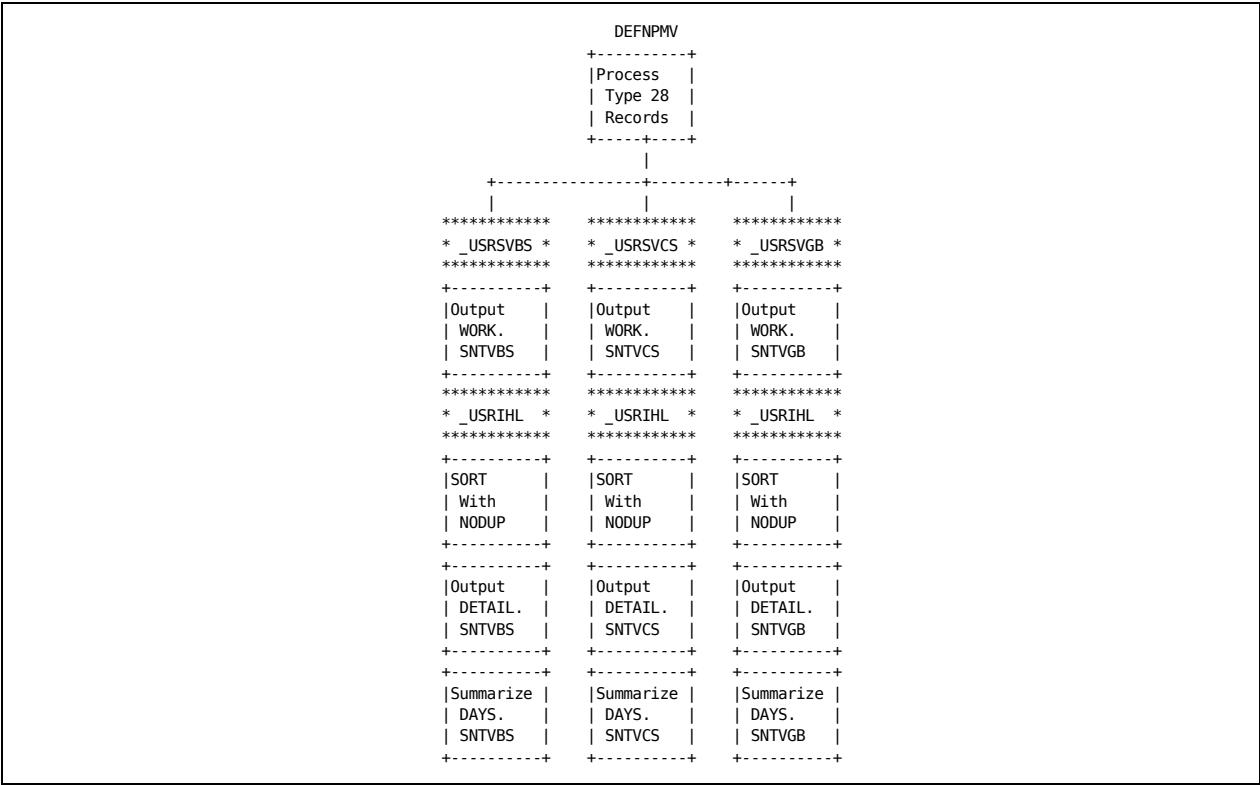
#### o Product Parameter-Related Exits

- SNTCIDRT - Link TP Circuit ID Definition Exit



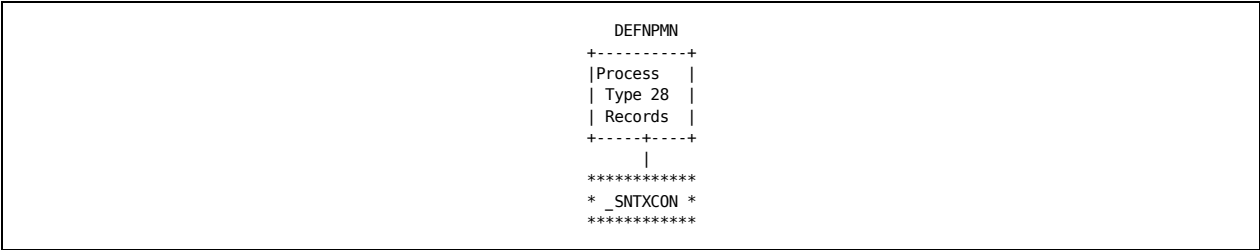
Note: All logic bounded by \*\*\*\*\* \*\*\*\*\* indicates a user routine or exit.

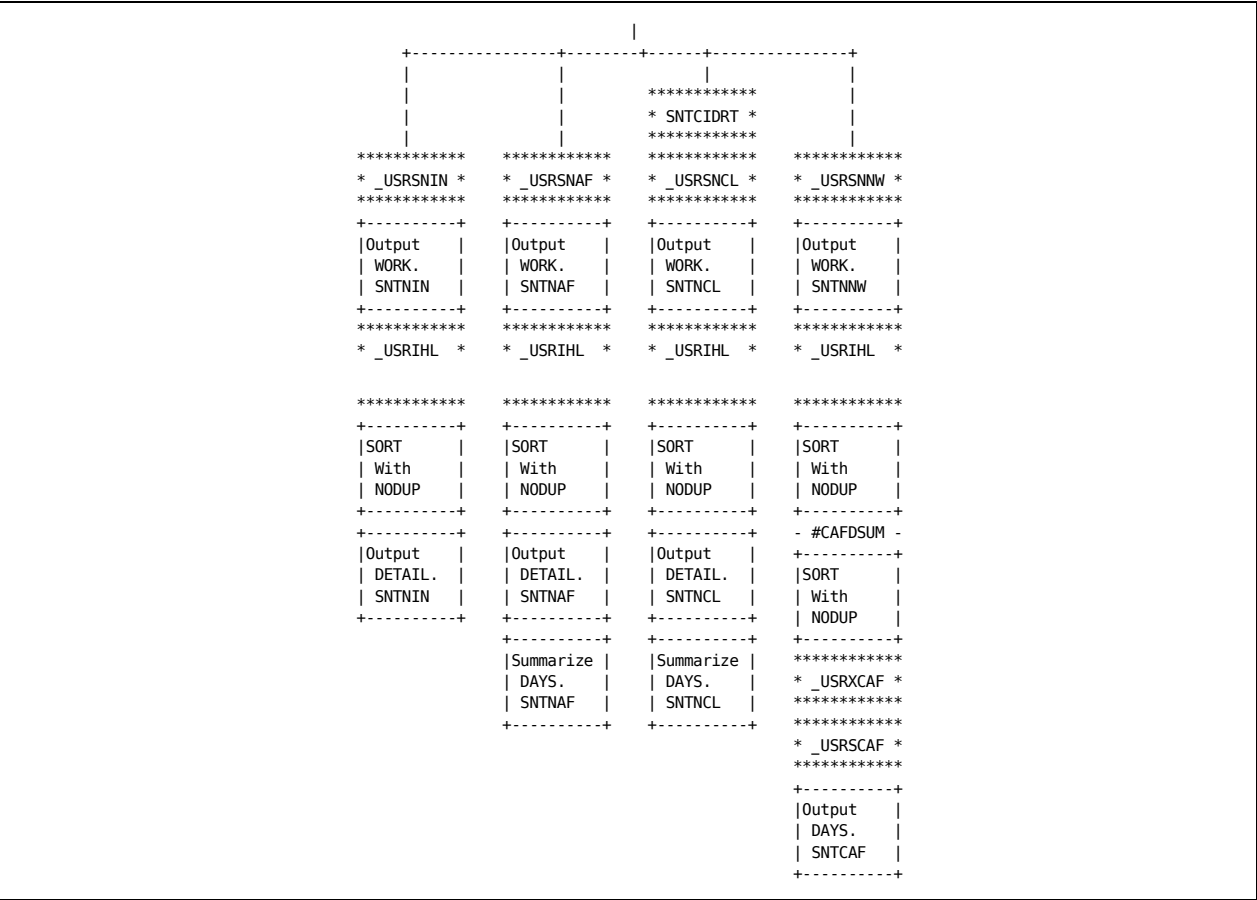
Figure 9-2. NPDA - Process Input Data into DETAIL/DAYS



Note: All logic bounded by \*\*\*\*\* \*\*\*\*\* indicates a user routine or exit.

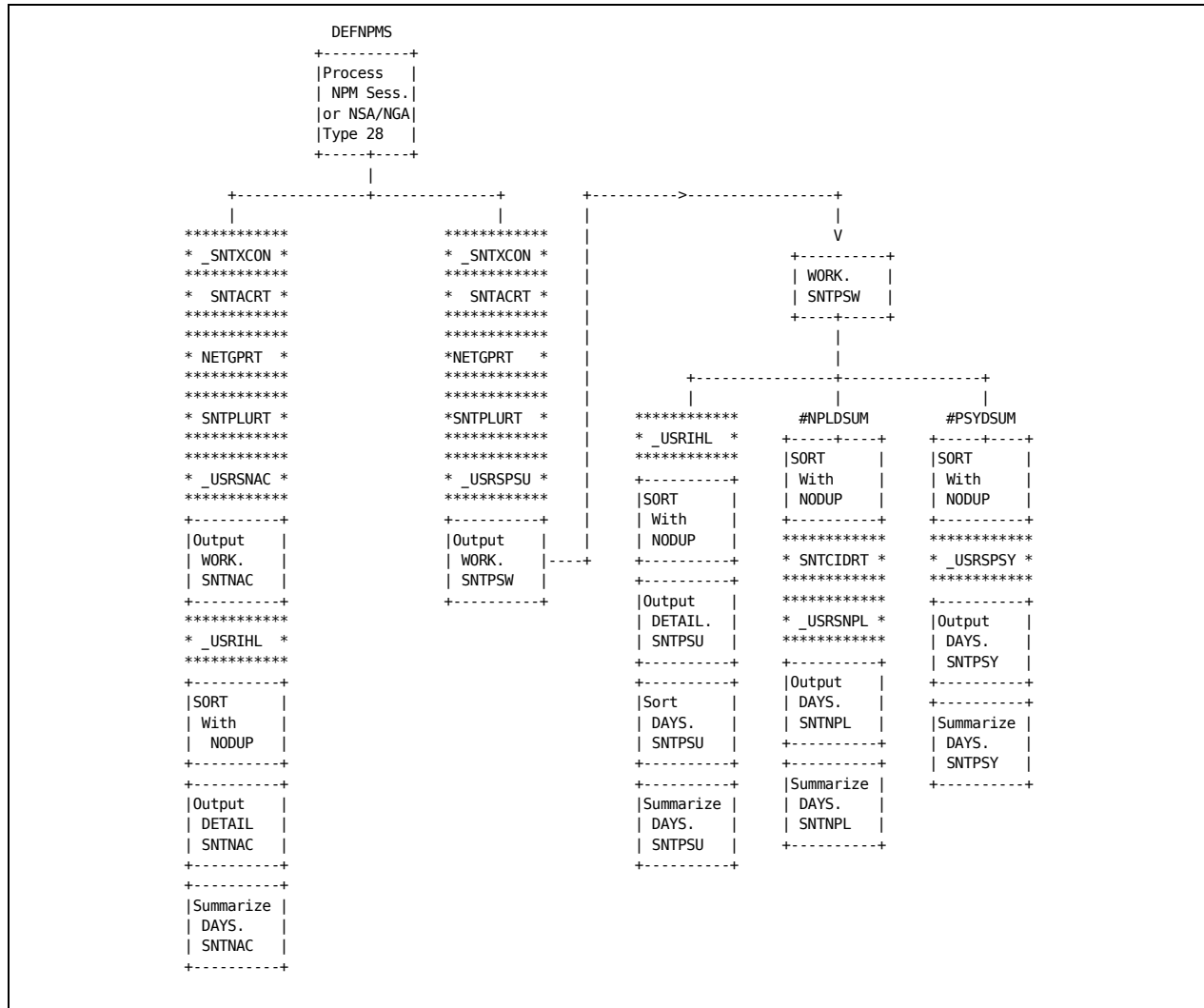
Figure 9-3. NPM VTAM Buffer and CSM - Process Input Data into DETAIL/DAYS





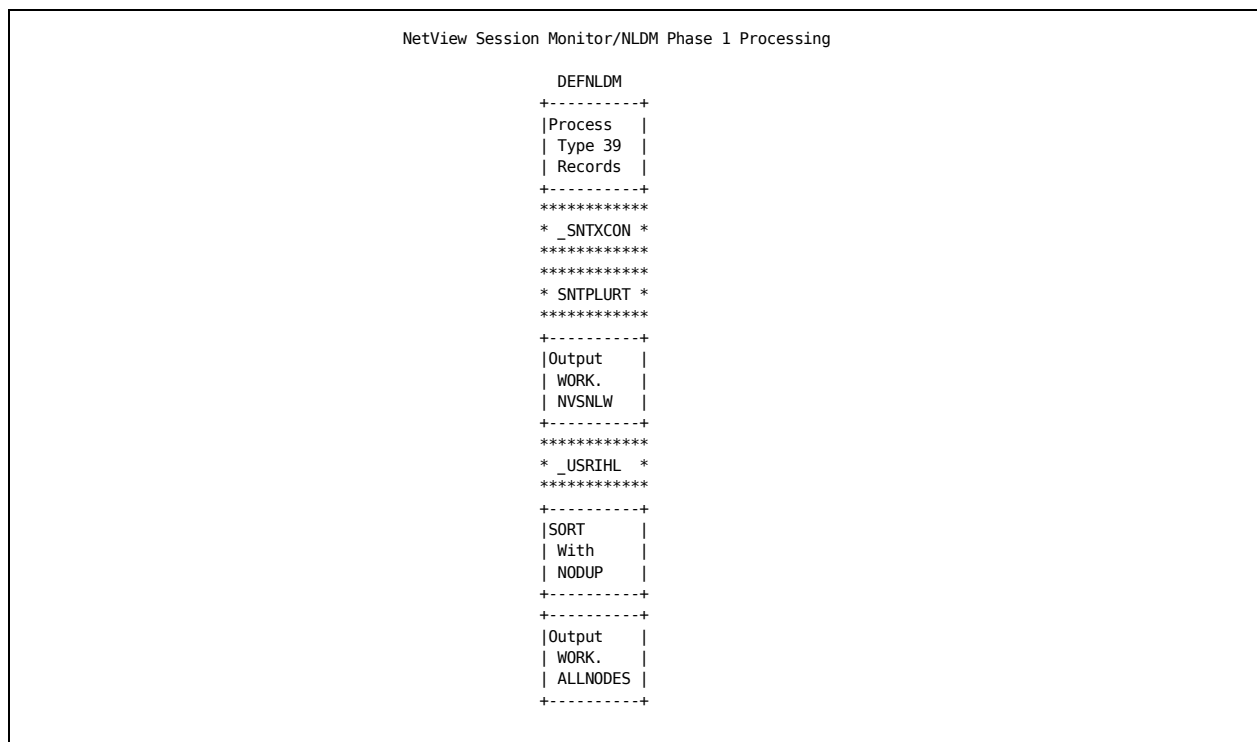
Note: All logic bounded by \*\*\*\*\* indicates a user routine or exit.

Figure 9-4. NPM Network - Process Input Data into DETAIL/DAYS



Note: All logic bounded by \*\*\*\*\* \*\*\*\*\* indicates a user routine or exit.

Figure 9-5. NPM Session and Network Session Accounting - Process Input Data into DETAIL/DAYS

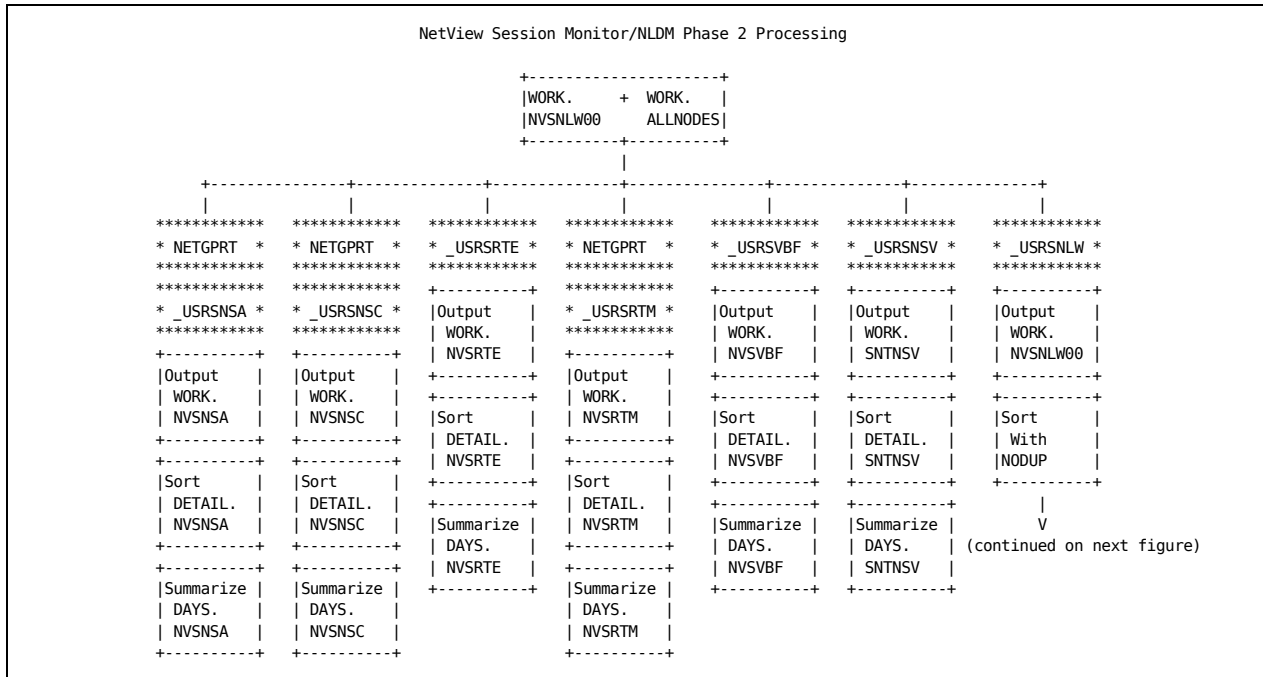




(cont'd on next figure)

Note: All logic bounded by \*\*\*\*\* \*\*\*\*\* indicates a user routine or exit.

Figure 9-6. NetView Session Monitor/NLDM - Process Input Data into DETAIL/DAYS (Part 1 of 3)



Note: All logic bounded by \*\*\*\*\* indicates a user routine or exit.

Figure 9-7. NetView Session Monitor/NLDM - Process Input Data into DETAIL/DAYS (Part 2 of 3)

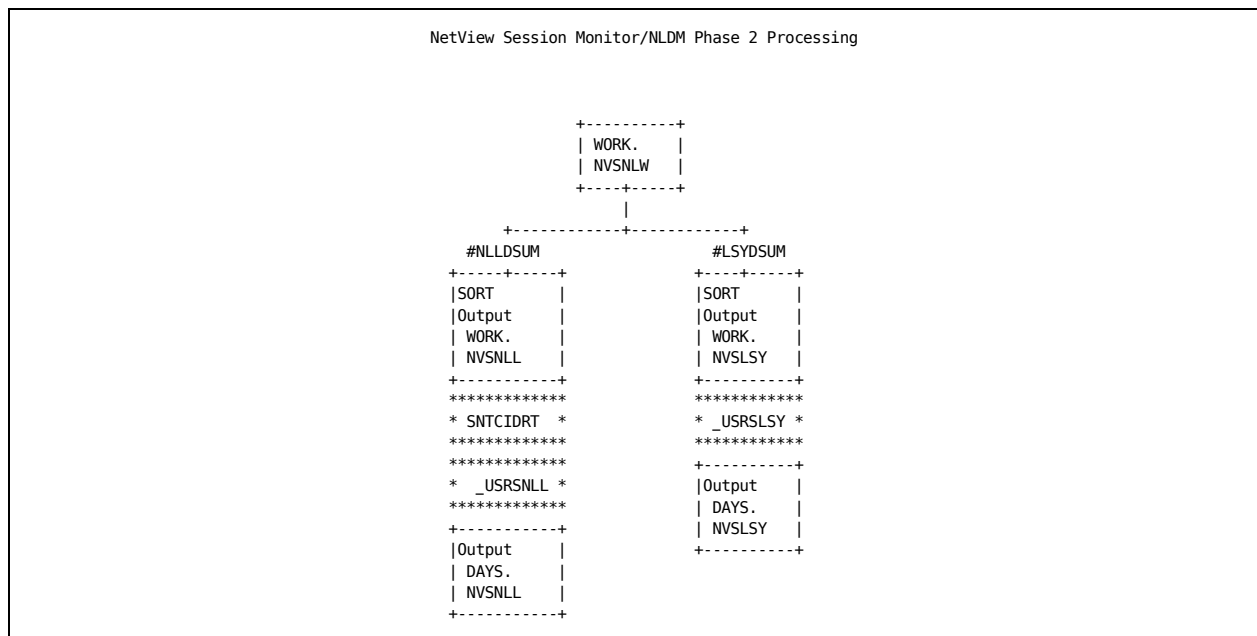




Figure 9-9. CA NetSpy - Process Input Data into DETAIL/DAYS

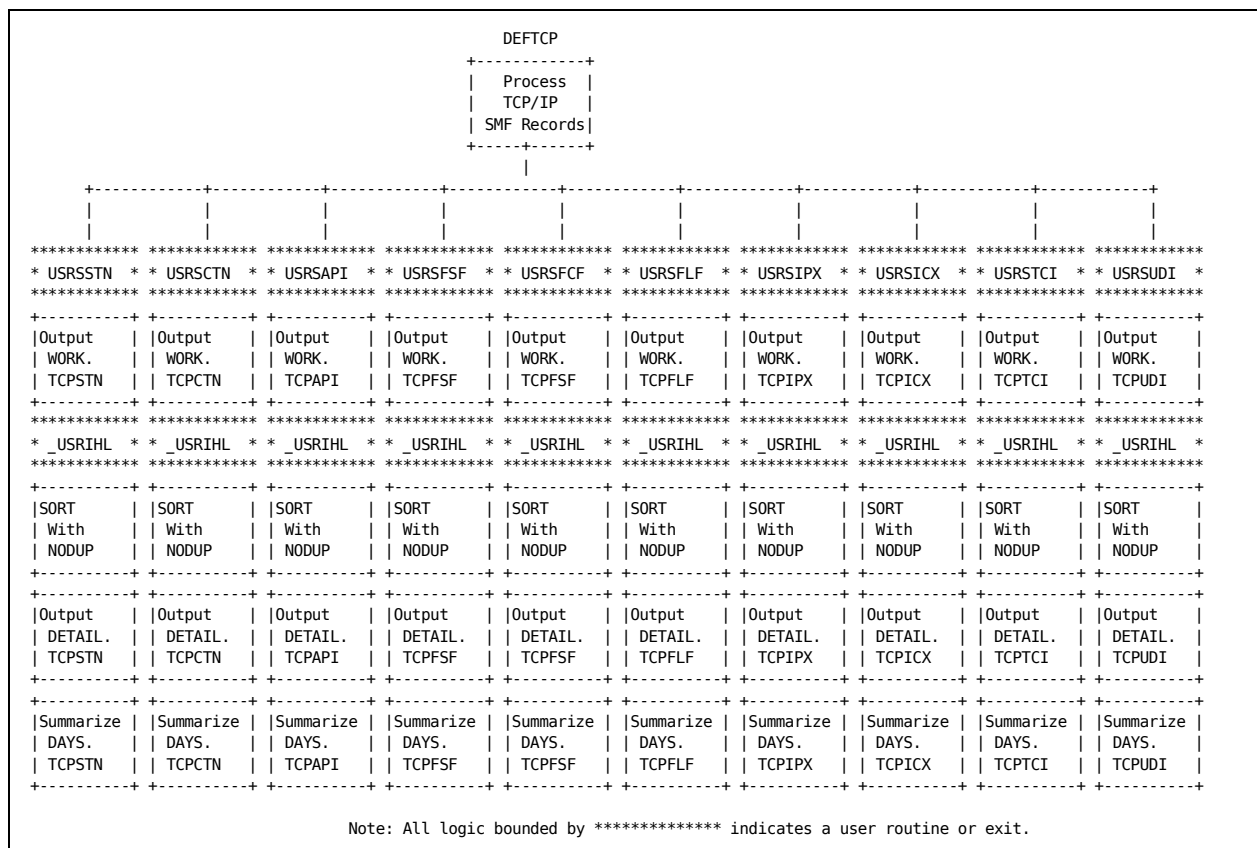


Figure 9-10. TCP/IP - Process Input Data into DETAIL/DAYS

Database Timespan Update

-----

Using the newly-created DETAIL or DAYS files, the DAYS, WEEKS, and MONTHS timespans are updated to retain the latest day, week-to-date, and month-to-date data.

There are no exit points provided in this phase.

File Aging

-----

CA MICS Network Analyzer Option files are aged to delete the oldest cycles and rename work files to current cycles.

There are no exit points provided in this phase.



# Chapter 10: MODIFICATION

---

At times, additional system customizing is needed to tailor CA MICS to meet your data center's needs. There are many user exit points provided within CA MICS. Each of these points corresponds to a position in the CA MICS logic where user modification:

- o Is likely to occur, based on our experience
- o Presents only a slight possibility of compromising CA MICS database or operational integrity
- o Is relatively easy to document and understand

Using the CA MICS exit facilities to augment processing logic is the safest method of system modification. Generally, we consider that the System Administrator has four levels or methods by which CA MICS can be augmented, changed, and enhanced:

- o CA MICS Standard Option and Parameter Definitions

The diverse installation and definition options provide most users with adequate provisions for customizing CA MICS.

- o Modification through User Exit Points

There may be site-dependent requirements that are not adequately addressed through the standard options and parameters of CA MICS. In these cases, one or more of the user exit points available to you may be used to code user-written routines that would satisfy these extended requirements.

- o Extension through Field-Developed Applications

Although most users do not at first consider this a way of modifying CA MICS, the development of field-developed applications may be the most advantageous way of addressing the need to modify a CA MICS product. For example, it may be better to write an application to handle additional SMF data than to attempt to modify the logic of the CA MICS Network Analyzer.

- o System Code Modification

As a last resort, you may be able to satisfy your site's



requirements by implementing a source code change.

This chapter explains the user exit points that are provided with the CA MICS Network Analyzer. You must carefully explore whether it is necessary to develop any user exit routines. To this end, you should first ensure that the requirement cannot be satisfied through one of the standard options or definitions. This process can be greatly facilitated by discussing the requirement with CA Technical Support.

**WARNING!** Before attempting to activate an exit, you should read and fully understand the information contained in Section 4.3 of the System Modification Guide, User Exit Facilities. The following material is intended to supplement, not replace, that discussion.

The design, coding, testing, and implementation of CA MICS user exit routines should be approached with caution as errors may result, causing the corruption of the data. You should be meticulous in the definition and validation of the exit routines to ensure that system integrity and performance have not been adversely affected.

This section contains the following topics:

[10.1 Available User Exits](#) (see page 1242)

[10.2 Exit Routine Considerations](#) (see page 1245)

[10.3 Input Exits](#) (see page 1246)

[10.4 Output Exits](#) (see page 1252)

[10.5 Implement Incremental Update](#) (see page 1287)

## 10.1 Available User Exits

There are two types of user exits that can be used to modify CA MICS logic: general exits and product exits. General exits apply to all the installed products. Product exits only apply to the product for which they are provided.

General exits allow user routines to be used for all products that process the raw SMF data. For more information on General Exits, see Chapter 4 of the System Modification Guide.

Product exits are classified according to their purpose and include input, work file, output, parameter-related, and accounting exits.

Input Exits are invoked as the raw input records are read. The CA MICS Network Analyzer provides the general input exit `_USRSEL`, which can be used to select or exclude data meeting special data-center-defined criteria, to add data elements, or to modify record fields as they are read. In addition, the general exit, `_USRIDL`, is provided at the end of input processing to permit examination of the CA MICS Input History Log SAS file, so that the user can terminate the DAILY run if critical data is missing from the run.

Work File Exits are provided for special work files that are created from raw input data for use in special processing. For example, they are used to create the DAYS timespan of a file when no DETAIL timespan is maintained.

Output Exit routines are invoked just before CA MICS writes an observation to the CA MICS database. Output exits are provided for each file and can be used to selectively block the writing of specified records, alter data elements in the records, or produce additional records for the target file or a user-defined file.

Parameter-related exits are also user exits, but are defined as part of the standard CA MICS installation process. They are normally associated with other parameters or options. For example, the Account Code Derivation Routine is a user exit routine for completing values for account codes that were defined in a separate but related member of `prefix.MICS.PARMS`, `SNTACRT`, the Account Code Definition parameter member. These exits are identified in this chapter, but are described in Chapter 7 of this guide.

Accounting Exits are identified in this chapter, but are

described in the Accounting and Chargeback User Guide.

The user exits for the CA MICS Network Analyzer are identified below:

o Product Input Exits

- \_USRSEL - File Processing Selection
- \_USRIHL - Examine Input History Log
- \_SNTXCON - Configuration Modification Exit

o Product Work File Exits

- \_USRSNLW - NLD Session Data Work File Exit
- \_USRSNNW - NPM Network Components Work File Exit

o Product Output Exits

- Direct exits:

These exits are provided as stub macros in sharedprefix.MICS.SOURCE. You can update these macros to manipulate observations before they are written out.

- \_USRSCAF - NPM Components Activity File Exit
- \_USRSNCL - NPM/NCP Link File Exit
- \_USRSNAF - NPM/NCP Activity File Exit
- \_USRSNEF - NPDA Event File Exit
- \_USRSNIN - NPM Incident File Exit
- \_USRSNPL - NPM Link Activity File Exit
- \_USRSNSF - NPDA Statistical File Exit
- \_USRSPSU - NPM User Activity File Exit
- \_USRSPSY - NPM System (PLU) Activity File Exit
- \_USRSVBS - VTAM Buffer Data File Exit
- \_USRSVCS - VTAM CSM Data File Exit
- \_USRSVGB - VTAM Global Data File Exit
- \_USRSNSV - NLD Session Service File Exit
- \_USRSLSY - NLD Session System (PLU) Activity File Exit
- \_USRSNSA - NLD Session Accounting File Exit
- \_USRSNSC - NLD Session Connectivity File Exit
- \_USRSNLL - NLD Session Link Activity File Exit
- \_USRSNLP - NCP Line Processor Activity File Exit
- \_USRSRTE - NLD Session Route File Exit
- \_USRSRTM - NLD Session Response Time File Exit
- \_USRSVBF - NLD Session VTAM Bind Failure File Exit
- \_USRSNSP - NetSpy PLU (Application) File Exit
- \_USRSNSS - NetSpy SLU (Terminal) File Exit
- \_USRSNVR - NetSpy Virtual Route Activity File Exit
- \_USRSNTS - Telnet Server Entry File Exit

- \_USRXCAF - SNTCAF DETAIL Timespan File Exit
- \_USRSNAC - NCP Network Accounting File Exit
- \_USRSLNF - LAN File Exit
- \_USRSGAF - Generic Alert File Exit

- Indirect exits:

These exits are defined by coding a SAS macro variable to indicate the name of a user source library member. For detailed information about coding exit routines, refer to Section 3.4 of the System Modification Guide.

- USRSNTS - Telnet Server Entry File Exit
- USRSSTN - Telnet Server File Exit
- USRSCTN - Telnet Client File Exit
- USRSFSF - FTP Server File Exit
- USRSFSF - FTP Client File Exit
- USRSAPI - API Calls for Sockets File Exit
- USRSFLF - FTP Login Failure File Exit
- USRTfff - DETAIL Tape Data Selection Exit

o Product Parameter-Related Exits

- SNTACRT - Network Account Code Derivation Exit
- SNTCIDRT- Link TP Circuit ID Definition Exit
- SNTNIDRT- Network Identifier Definition Exit
- SNTPLURT- PLU (Application) Processing Exit
- NETGPRT - Network Service Group Definition Exit

o Accounting Exits

- \_USRJNAC - NCP Network Accounting File Accounting Exit
- \_USRJPSU - NPM User Activity File Accounting Exit
- \_USRJNSS - NetSpy User Activity File Accounting Exit
- \_USRJNTS - Telnet Server Entry File Accounting Exit
- \_USRJUNC - NLDM Session Connectivity File Acctg Exit
- \_USRJUNA - NLDM Session Accounting File Acctg Exit
- \_USRJURT - NLDM Response Time File Accounting Exit
- \_USRJURT - NLDM Response Time File Accounting Exit

## 10.2 Exit Routine Considerations

There are data elements available for use by the user exits that vary according to the processing phase and the particular user exit point. Special data elements that are used in the CA MICS Network Analyzer update process but are not stored in the CA MICS database (and, therefore, have no corresponding Data Dictionary descriptions) are identified below. The individual user exit descriptions list which of these elements are available for the user exit routine.

ROUTINE - Name of the Invoking Routine

FILEID - Identifier of the File Being Processed

SMFRTYPE - SMF Record Type of the Record Being Processed

NPMSYSID - NPM Session Statistics Data System Identifier

COMPT - 8-Character Product and Data Source Identifier

## 10.3 Input Exits

This section provides a description of the user exits that are invoked during the first phase of the CA MICS Network Analyzer Option DAILY update processing. The exits are listed alphabetically.

Each exit description includes the name and title, a description of its purpose, when it is invoked, and whether it has an interface to the CA MICS Accounting and Chargeback Option. It also shows which data elements are available, the special considerations to note, and a sample user exit.

```
+-----+
| _ U S R S E L | File Processing Selection Exit
+-----+
```

**DESCRIPTION:** This exit allows access to each record processed, including SMF type 28, 37, 39, 118, 119, and user-defined CA NetSpy records.

**INVOCATION:** The exit gains control after a detail input record has been read and before the network ID assignment routine, SNTNIDRT, has been invoked.

**ACCOUNTING INTERFACE:** No interface to CA MICS Accounting and Chargeback Option.

**USES:** This exit can be used to delete records before processing or to modify a 4-character ORGSYSID.

**ELEMENTS AVAILABLE:**

**ROUTINE** - The name of the routine that invoked this exit.

To use this exit in the CA MICS Network Analyzer Option process, test for ROUTINE = 'DYSNTFMT'.

**SMFRTYPE** - The record type of the input record:

- 28 - NPM Session and Network Data Record
- 37 - NPDA Report Record
- 39 - NLDM External Log Record
- 118 - TCP/IP SMF Record
- 119 - TCP/IP SMF Record

**NSPYRTPE** - CA NetSpy Record (user-defined; specified on the INPUTSOURCE statement in SNTGENIN)

ORGSYSID - Original SYSID from SMF record

ENDTS - Time when record was written to SMF

CODING RESTRICTIONS: Refer to the System Modification Guide, Section 4.3.2.

SPECIAL NOTES:

1. This exit is part of the CA MICS platform and is located in `sharedprefix.MICS.SOURCE(#BASEXIT)`. However, it is recommended that the user modify `prefix.MICS.USER.SOURCE(#BASEXIT)`. A more detailed description of this routine is provided in the System Modification Guide, Section 4.3.2, Types of CA MICS Exits.
2. Because this exit is used in many places, it is necessary to qualify all coding in this exit by examining the name of the routine in which the exit was invoked. The program variable `ROUTINE` exists for this purpose. See the example below.
3. `NETWRKID` is not set until after this exit has been processed.
4. No time offset has been applied to `ENDTS` when this exit gains control.

SAMPLE USER EXIT:

In this exit, the `ORGSYSID` value of `SYST` or `SYSX` found in the raw input is translated to `TEST`.

MACRO \_USRSEL

```
IF ROUTINE = 'INPUTRDR' THEN DO;
 /* exit routine code here for INPUTRDR */
END;
IF ROUTINE = 'DYSNTFMT' THEN DO;
 IF ORGSYSID = 'SYST' OR ORGSYSID = 'SYSX' THEN
 ORGSYSID = 'TEST';
END;
%
```

```
+-----+
| _ U S R I H L | Examine Input History Log Exit
+-----+
```

**DESCRIPTION:** This exit permits inspection of the DETAIL timespan checkpoint SAS file immediately following processing of all input records.

**INVOCATION:** This exit is referenced in code that passes the DETAIL timespan checkpoint SAS file. This code reads \_ADMX.CKPTDATA as an integrity check on that file, and in the process allows the user to inspect the file's contents.

**ACCOUNTING INTERFACE:** No interface to CA MICS Accounting and Chargeback Option.

**USES:** This exit can be used to abort daily update processing based on an extended checkpoint examination algorithm. For example, the daily process will end normally if data from one or more of the sources (NPM/Network, NPM/Session, NLDM/RTM, NPDA, CA NetSpy, or TCP/IP) is provided. However, it may be critical that data from at least two of the sources is provided for a successful update or data from two or more systems is in the update process. This routine can be used to examine all entries in \_ADMX.CKPTDATA to test for the required condition. If the appropriate data is not found, the CA MICS DAILY step could be terminated with an ABORT abend statement.

**ELEMENTS AVAILABLE:**

All elements in the ADMIHL File

**CODING RESTRICTIONS:** Refer to the System Modification Guide Section 4.3.2.1.

**SPECIAL NOTES:**

1. This exit is part of the CA MICS platform and is located in sharedprefix.MICS.SOURCE(#BASEXIT). However, it is recommended that the user modify prefix.MICS.USER.SOURCE(#BASEXIT). A more detailed description of this routine is provided in the System Modification Guide, Section 4.3.2, Types of CA MICS Exits.
2. Because this exit is used in many places, it is necessary to qualify all coding in this exit by examining the name of the routine in which the exit was invoked. Use the program variable ROUTINE. See the example below.



3. Note that COMPT has a special meaning to the CA MICS Network Analyzer Option, since it not only identifies the product but also each data source, as follows:

```
'SNT NPDA' - NetView or CA NetMaster SMF Record Type 37
'SNT NPMN' - NPM Network data SMF Record Type 28
'SNT NPMS' - NPM Session data SMF Record Type 28
'SNT NLDM' - NetView or CA NetMaster SMF Record Type 39
'SNT NSPY' - CA NetSpy User-Defined SMF Record Type
'SNT TCP ' - TCP/IP for z/OS data SMF Record Type
118-119
```

#### SAMPLE USER EXIT:

In this sample exit, the Input History Log is examined to determine if input for NLDM and NPM Session data was received for the production SYSID 'TST1'. When End of File (EOF) is reached for the DAILY update run, a check is done to determine if both input sources were provided. If either data source was not provided, then further DAILY processing is aborted and messages are written specifying which data was not present.

```
MACRO _USRIHL
 IF ROUTINE = 'DYSNTFMT' THEN DO;
 RETAIN TST1NLDM TST1NPMS 0;
 IF SYSID = 'TST1' THEN DO;
 IF COMPT = 'SNT NLDM' THEN TST1NLDM = 1;
 IF COMPT = 'SNT NPMS' THEN TST1NPMS = 1;
 END;
 IF EOF THEN DO;
 IF TST1NLDM AND TST1NPMS THEN GOTO ENDCHECK;
 IF TST1NLDM THEN DO;
 PUT 'NPM SESSION DATA MISSING FROM UPDATE';
 END;
 ELSE DO;
 PUT 'NLDM/RTM DATA MISSING FROM UPDATE';
 END;
 ABORT ABEND;
END;
ENDCHECK:
END;
%
```

```
+-----+
| _ S N T X C O N | Configuration Modification Exit
+-----+
```

**DESCRIPTION:** This exit allows you to modify the configuration data contained in NPM, CA NetSpy, NetView, and CA NetMaster data.

**INVOCATION:** This exit is linked from the SNTNLD3 module for NetView and CA NetMaster data, from the SNTNSINP module for CA NetSpy data.

**ACCOUNTING INTERFACE:** No interface to CA MICS Accounting and Chargeback Option.

**USES:** This exit can be used to modify any of the configuration data provided in the CA NetSpy, NPM, NetView, or CA NetMaster data. Generally, there will be no need to modify the configuration data presented by the network monitor products supported by CA MICS. However, it is possible for a particular physical resource to be known by more than one name over time, such as an NCP whose name is changed with each regeneration to reflect the generation level. Because the CA MICS Network Analyzer Option summarizes information for each resource and session based on the logical names of the configuration elements, changing the logical name of an NCP, for example, causes the information for the specific resource to no longer be summarized into a single CA MICS Network Analyzer Option observation in the higher timespans.

This problem can be circumvented by using the \_SNTXCON exit to rename the affected configuration elements back to a common name.

**ELEMENTS AVAILABLE:**

All configuration elements. See the individual CA MICS Network Analyzer Option file descriptions in Chapter 5 for more information on the available configuration elements.

**CODING RESTRICTIONS:** Refer to the System Modification Guide Section 4.3.2.

**SPECIAL NOTES:**

1. This exit is part of the CA MICS Network Analyzer Option and is located in `sharedprefix.MICS.SOURCE(#SNTEXIT)`. However, it is recommended that the user modify `prefix.MICS.USER.SOURCE(#SNTEXIT)`.
2. Because this exit is used in many places, it is necessary to qualify all coding in this exit by

examining the name of the routine in which the exit was invoked. The program variable ROUTINE exists for this purpose. See the example below.

3. Note that COMPT has a special meaning to the CA MICS Network Analyzer Option, since it not only identifies the product but also identifies each data source, as follows:

'SNT NPDA' - NetView or CA NetMaster SMF Record Type 37  
'SNT NPMN' - NPM Network data SMF Record Type 28  
'SNT NPMS' - NPM Session data SMF REcord Type 28  
'SNT NLDM' - NetView or CA NetMaster SMF Record Type 39  
'SNT NSPY' - CA NetSpy User-Defined SMF Record Type  
'SNT TCP ' - TCP/IP for z/OS data SMF Record Type  
118-119

#### SAMPLE USER EXIT:

In this sample exit, a site routinely changes the names of the NCP subarea nodes each time a new NCP gen is run to reflect the NCP generation version number. For example, for subarea 29, the NCP name is of the form N29001, N29002, N29003, and so forth. In order to be able to track activity related to NCP subarea 29 over time, the following \_SNTXCON exit sample will change any value of the SLUSAPU data element (SLU subarea name) that begins with N29 to just N29.

```
MACRO _SNTXCON
 IF COMPT EQ 'SNT NPMN' OR COMPT EQ 'SNT NPMS' THEN DO;
 IF SLUSAPU EQ : 'N29' THEN SLUSAPU='N29';
 END;
%
```

## 10.4 Output Exits

This section provides an in-depth description of the CA MICS Network Analyzer Option standard output processing exits that are invoked during phases 1 and 2 of the DAILY update processing flow. The exits are organized alphabetically.

Each exit description includes the user exit name and title, a description of its purpose, when it is invoked, and whether it has an interface to the CA MICS Accounting and Chargeback Option. It also shows what data elements are available, any special considerations, and a sample user exit.

```
+-----+
| _ U S R S C A F | NPM Components Activity File Exit
+-----+
```

**DESCRIPTION:** This exit allows access to the data elements used to build the observations in the NPM Components Activity File.

**INVOCATION:** Exit gains control immediately prior to the output of the observation to the NPM Components Activity File in the #CAFDSUM routine.

**ACCOUNTING INTERFACE:** No interface to CA MICS Accounting and Chargeback Option.

**USES:** This exit is used to add or change data elements, or to delete observations from the NPM Components Activity File. This file is built from the SMF Type 28 Record or the user-defined CA NetSpy SMF record.

**ELEMENTS AVAILABLE:**

- All elements in the NPM Components Activity File
- All elements in the SMF Type 28 Record
- All elements in the user-defined CA NetSpy SMF record

**CODING RESTRICTIONS:** See the System Modification Guide, Section 4.3.

**SPECIAL NOTE:**

To implement this exit at the unit level, code it in prefix.MICS.USER.SOURCE(#SNTEXTIT).

**SAMPLE USER EXIT:**

In this sample exit, data produced while testing a new NCP is blocked from the CA MICS database. If NCPNAME equals NCPTEST, the variable SKIP\_REC is set to ONE and the current observation is deleted (that is, it is not written to the CA MICS database).

```
MACRO _USRSCAF
 IF NCPNAME = 'NCPTEST' THEN SKIP_REC = ONE;
 %
+-----+
| _ U S R S L S Y | NLDM System (PLU) Activity File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the NLDM System (PLU) Activity File.

INVOCATION: Exit gains control immediately prior to the output of records to the NLDM System Activity File in the #LSYDSUM routine.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the NLDM System Activity File. This file is built from the NLDM session data work file, which produces both the NLDM System Activity File and the NLDM Link File.

ELEMENTS AVAILABLE:

All elements in the NLDM System (PLU) Activity File

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

SPECIAL NOTE:

To implement this exit at the unit level, code it in prefix.MICS.USER.SOURCE(#SNTEXIT).

SAMPLE USER EXIT:

To limit DASD requirements for this file, you may want to eliminate sessions with very small values. In this sample, any session with less than five total responses or less than 200 bytes of transferred data is deleted because it is not useful for reporting purposes.

You can use this user exit to provide those filtering capabilities.

```
MACRO _USRSLSY
 IF LSYTRES LT 5 OR
 SUM(LSYNRTBS,LSYNRTBR,LSYNRCBS,LSYNRCBR) LT 200 THEN
 SKIP_REC=ONE;
```

%

+-----+

| \_ U S R S N A F | NPM/NCP Activity File Exit

+-----+

DESCRIPTION: This exit allows access to the data elements used to build the records in the NPM/NCP Activity File.

INVOCATION: Exit gains control immediately prior to the output of records to the NPM/NCP Activity File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the NPM/NCP Activity File. This file is built from the SMF Type 28 Record (NPM Network Log Record) or the user-defined CA NetSpy SMF record, which can also be processed by the exit routine.

ELEMENTS AVAILABLE:

- All elements in the NPM/NCP Activity File
- All elements in the SMF Type 28 Record
- All elements in the user-defined CA NetSpy SMF record

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

SPECIAL NOTE:

To implement this exit at the unit level, code it in prefix.MICS.USER.SOURCE(#SNTEXTIT).

SAMPLE USER EXIT:

In this sample exit, if the logical SYSID is TST1 and the NCPNAME is NCPND01, then SKIP\_REC is set to ONE and the observation is deleted (that is, it is not written to the CA MICS database).

```

MACRO _USRSNAF
 IF SYSID = 'TST1' THEN
 IF NCPNAME = 'NCPND01' THEN SKIP_REC = ONE;
 %
+-----+
| _ U S R S N C L | NPM/NCP Link File Exit
+-----+

```

DESCRIPTION: This exit allows access to the data elements used to build the records in the NPM/NCP Link File.

INVOCATION: Exit gains control immediately prior to the output of records to the NPM/NCP Link File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the NPM/NCP Link File. This file is built from the SMF type 28 record or the user-defined CA NetSpy SMF record, which can also be processed by the exit routine.

#### ELEMENTS AVAILABLE:

- All elements in the NPM/NCP Link File
- All elements in the SMF Type 28 Record
- All elements in the user-defined CA NetSpy SMF record

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

#### SPECIAL NOTE:

To implement this exit at the unit level, code it in prefix.MICS.USER.SOURCE(#SNTEXTIT).

#### SAMPLE USER EXIT:

In this sample exit, a check for Link Name LN061239 is performed. If it is found, LINKSPD is overridden with a new value. The sending link speed is set equal to LINKSPD and the receiving link speed is set to 0. The four percent busy calculations for sending, receiving, retransmission, and total percent link busy are recalculated using the new speed.

```

MACRO _USRSNCL
 IF NETNAME = 'LN061239' THEN DO;

```

```
LINKSPD = 4800;
NCLNRSLS = 4800;
NCLNRRLS = 0;
/* RECALCULATE PERCENT LINK BUSY */
NCLPCLBS=(SUM(OF NCLNRCHR,NCLNRCHS) /
((LINKSPD/8) * DURATION)) * HUN;
/* RECALCULATE PERCENT LINK BUSY SENDING */
NCLPCSLB=((NCLNRCHS) /
((NCLNRSLS/8) * DURATION))*HUN;
/* RECALCULATE PERCENT LINK BUSY RECEIVING */
NCLPCRLB=((NCLNRCHR) /
((NCLNRSLS/8) * DURATION))*HUN;
/* RECALCULATE PERCENT LINK BUSY RETRANSMISSION */
NCLPCELB=((NCLNRBY) /
((NCLNRSLS/8) * DURATION))*HUN;
END;
%
```

+-----+  
| \_ U S R S N E F | - NPDA Event File Exit  
+-----+

DESCRIPTION: This exit allows access to the data elements used to build the records in the NPDA Event File.

INVOCATION: Exit gains control immediately prior to the output of records to the NPDA Event File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the NPDA Event File. This file is built from the SMF Type 37 Record (NPDA Report Record), which can also be processed by the exit routine.

ELEMENTS AVAILABLE:

All elements in the NPDA Event File  
All elements in the SMF Type 37 Record

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

SPECIAL NOTE:

To implement this exit at the unit level, code it in prefix.MICS.USER.SOURCE(#SNTEXTIT).

SAMPLE USER EXIT:



In this sample exit, a check is performed to determine if the NPM General Event Cause Code is undefined (for example, equal to 'FF'). If so, SKIP\_REC is set to ONE and the observation is deleted (that is, it is not written to the CA MICS database).

```
MACRO _USRSNEF
 IF NEFGEVCC = 'FF' THEN SKIP_REC = ONE;
 %
+-----+
| _ U S R S N I N | Network Incident File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the Network Incident File.

INVOCATION: Exit gains control immediately prior to the output of records to the Network Incident File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the Network Incident File. This file is built from the SMF Type 28 Record (NPM Network Log Record) and the CA NetSpy subtype X record (General Alert).

#### ELEMENTS AVAILABLE:

- All elements in the Network Incident File
- All elements in the SMF Type 28 Record
- All elements in the CA NetSpy Type X Record

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

#### SPECIAL NOTE:

To implement this exit at the unit level, code it in prefix.MICS.USER.SOURCE(#SNTEXTIT).

#### SAMPLE USER EXIT:

In this sample exit, if the exception code is 101, which indicates that network component traffic has exceeded a data-center-defined threshold, the low limit criteria value is examined. This value was accidentally set to 40 during testing, resulting in the generation of a large number of

meaningless NPM monitor exception records. The user exit code tests for an exception value of less than 4000, preventing records from being written to the CA MICS database when this condition is met.

```
MACRO _USRSNIN
 IF NINCODE = 101 THEN DO;
 IF NINNRHIC < 4000 then SKIP_REC = ONE;
 END;
```

```
+-----+
| _ U S R S N L P | NCP Line Processor Activity File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the NCP Line Processor Activity File.

INVOCATION: Exit gains control immediately prior to the output of records to the NCP Line Processor Activity File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the NCP Line Processor Activity File.

ELEMENTS AVAILABLE:

All elements in the NCP Line Processor Activity File.

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

SPECIAL NOTE:

To implement this exit at the unit level, code it in prefix.MICS.USER.SOURCE(#SNTEXTIT).

SAMPLE USER EXIT:

In this sample exit, if the logical SYSID equals TEST, then SKIP\_REC is set to ONE and the observation is deleted (that is, it is not written to the CA MICS database).

```
MACRO _USRSNLP
 IF SYSID = 'TEST' THEN SKIP_REC = ONE;
%
```

```
+-----+
| _ U S R S N L L | NLDM Link Activity File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the NLDM Link Activity File.

INVOCATION: Exit gains control immediately prior to the output of records to the NLDM Link Activity File in the #NLLDSUM routine.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the NLDM Link Activity File. This file is built from the NLDM session data work file.

ELEMENTS AVAILABLE:

All elements in the NLDM Link Activity File

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

SPECIAL NOTE:

To implement this exit at the unit level, code it in prefix.MICS.USER.SOURCE(#SNTEXTIT).

SAMPLE USER EXIT:

In this sample exit, if the logical SYSID equals TEST, then SKIP\_REC is set to ONE and the observation is deleted (that is, it is not written to the CA MICS database).

```
MACRO _USRSNLL
 IF SYSID = 'TEST' THEN SKIP_REC = ONE;
%
```

```
+-----+
| _ U S R S N P L | NPM Link Activity File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the NPM Link Activity File.

INVOCATION: Exit gains control immediately prior to the output of records to the NPM Link Activity File in the

#NPLDSUM routine.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the NPM Link Activity File. This file is built from the DETAIL timespan of the NPM User Activity File. Input record processing for the NPM Session Statistics DETAIL File can be performed in the \_USRSEL exit or the \_USRSPSU exit.

ELEMENTS AVAILABLE:

All elements in the NPM Link Activity File  
All elements in the NPM User Activity File

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

SPECIAL NOTE:

To implement this exit at the unit level, code it in prefix.MICS.USER.SOURCE(#SNTEXTIT).

SAMPLE USER EXIT:

In this sample exit, if the logical SYSID equals TEST, then SKIP\_REC is set to ONE and the observation is deleted (that is, it is not written to the CA MICS database).

```
MACRO _USRSNPL
 IF SYSID = 'TEST' THEN SKIP_REC = ONE;
%
```

```
+-----+
| _ U S R S N S A | NLDM Session Accounting File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the NLDM Session Accounting File.

INVOCATION: Exit gains control immediately prior to the output of records to the NLDM Session Accounting File.

ACCOUNTING INTERFACE: This exit contains complex-level code and is used by the CA MICS Accounting and Chargeback Option. To use this file exit for user-specified modifications, see Section 4.3 of the System Modification Guide.

USES: This exit is used to add, change, or delete data elements or observations from the NLDM Session Accounting File. This file is built from the SMF Type 39 Record (NetView or NLDM External Log Record), which can also be processed by the exit routine.

#### ELEMENTS AVAILABLE:

All elements in the NLDM Session Accounting File  
All elements in the SMF Type 39 Record

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

#### SPECIAL NOTE:

To implement this exit at the unit level, code it in prefix.MICS.USER.SOURCE(#SNTEXTIT).

#### SAMPLE USER EXIT:

In this sample exit, if the total bytes transmitted for any observation in this session is less than 200, the observation is deleted.

USER EXIT EXAMPLE #1: The CA MICS Accounting and Chargeback Option is not installed in the database unit.

```
MACRO _USRSNSA
 IF SUM(NSANRCBS,NSANRCBR,NSANRTBS,NSANRTBR) LT 200 THEN
 SKIP_REC = ONE;
%
```

USER EXIT EXAMPLE #2: The CA MICS Accounting and Chargeback Option is installed in the database unit.

Note that even the observations deleted by this exit, pass through the accounting functions/calculations before being deleted.

```
MACRO _USRSNSA
 _USRUNSA _USRJNA
 IF SUM(NSANRCBS,NSANRCBR,NSANRTBS,NSANRTBR) LT 200 THEN
 SKIP_REC = ONE;
%
```

```
+-----+
| _ U S R S N S C | NLDM Session Connectivity File Exit
+-----+
```

**DESCRIPTION:** This exit allows access to the data elements used to build the records in the NLDM Session Connectivity File.

**INVOCATION:** Exit gains control immediately prior to the output of records to the NLDM Session Connectivity File.

**ACCOUNTING INTERFACE:** This exit contains complex-level code and is used by the CA MICS Accounting and Chargeback Option. To use this file exit for user-specified modifications, see Section 4.3 of the System Modification Guide.

**USES:** This exit is used to add, change, or delete data elements or observations from the NLDM Session Connectivity File. This file is built from the SMF Type 39 Record (NetView or NLDM External Log Record), which can also be processed by the exit routine.

**ELEMENTS AVAILABLE:**

- All elements in the NLDM Session Accounting File
- All elements in the SMF Type 39 Record

**CODING RESTRICTIONS:** See the System Modification Guide, Section 4.3.

**SPECIAL NOTE:**

- To implement this exit at the unit level, code it in prefix.MICS.USER.SOURCE(#SNTEXTIT).

**SAMPLE USER EXIT:**

In this sample exit, if PLDOMAIN is equal to TL080134, the session occurred on the z/OS test system and the observation can be deleted.

**USER EXIT EXAMPLE #1:** CA MICS Accounting and Chargeback Option is not installed in the database unit.

```
MACRO _USRSNSC
 IF PLDOMAIN='TL080134' THEN SKIP_REC=ONE;
%
```

**USER EXIT EXAMPLE #2:** CA MICS Accounting and Chargeback Option is installed in the database unit.

Note that even the observations deleted by this exit, pass

through the accounting functions/calculations before being deleted.

```
MACRO _USRSNSC
 _USRUNSC _USRJNC
 IF PLDOMAIN='TL080134' THEN SKIP_REC=ONE;
 %
+-----+
| _ U S R S N S F | NPDA Statistical File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the NPDA Statistical File.

INVOCATION: Exit gains control immediately prior to the output of records to the NPDA Statistical File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the NPM Statistical File. This file is built from the SMF Type 37 Record (NPDA Report Record), which can also be processed by the exit routine.

ELEMENTS AVAILABLE:

```
All elements in the NPDA Statistical File
All elements in the SMF Type 37 Record
```

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

SPECIAL NOTE:

```
To implement this exit at the unit level, code it in
prefix.MICS.USER.SOURCE(#SNTEXTIT).
```

SAMPLE USER EXIT:

In this exit, if the failing resource name is CHCAU1, then SKIP\_REC is set to ONE and the observation is deleted (that is, it is not written to the CA MICS database).

```
MACRO _USRSNSF
 IF NSFFRNAM = 'CHCAU1' THEN SKIP_REC = ONE;
 %
+-----+
| _ U S R S N S P | NetSpy PLU (Application) File Exit
```

+-----+

DESCRIPTION: This exit allows access to the data elements used to build the records in the CA NetSpy PLU (Application) File.

INVOCATION: Exit gains control immediately prior to the output of records to the CA NetSpy PLU (Application) File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the CA NetSpy PLU (Application) File. This file is built from the user-defined CA NetSpy SMF record type.

ELEMENTS AVAILABLE:

All elements in the CA NetSpy PLU (Application) File  
All elements in the user-defined CA NetSpy SMF records

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

SPECIAL NOTE:

To implement this exit at the unit level, code it in prefix.MICS.USER.SOURCE(#SNTEXTIT).

SAMPLE USER EXIT:

In this sample exit, if the first three characters of the PLU (application) name are not TSO or IMS, then SKIP\_REC is set to ONE and the observation is deleted (that is, it is not written to the CA MICS database).

```
MACRO _USRSNSP
 TEMPPLU= SUBSTR(PLU,1,3);
 IF TEMPPLU NE 'TSO' AND TEMPPLU NE 'IMS'
 THEN SKIP_REC = ONE;
%
```

+-----+

| \_ U S R S N S S | NetSpy SLU (Terminal) File Exit

+-----+

DESCRIPTION: This exit allows access to the data elements used to build the records in the CA NetSpy SLU (Terminal) File.



INVOCATION: Exit gains control immediately prior to the output of records to the CA NetSpy SLU (Terminal) File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the CA NetSpy SLU (Terminal) File. This file is built from the user-defined CA NetSpy SMF record type.

ELEMENTS AVAILABLE:

All elements in the CA NetSpy SLU (Terminal) File  
All elements in the user-defined CA NetSpy SMF records

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

SPECIAL NOTE:

To implement this exit at the unit level, code it in prefix.MICS.USER.SOURCE(#SNTEXTIT).

SAMPLE USER EXIT:

In this sample exit, the site has a naming convention that column 4 of the SLU value uses to identify whether a terminal is locally attached, the site wants to exclude those devices from the NSS file. The fourth position of the SLU is checked and, if it denotes a locally-attached terminal, the observation is deleted.

```
MACRO _USRSNSS
 IF SUBSTR(4,1) EQ 'L' THEN SKIP_REC=ONE;
 %
+-----+
| _ U S R S N S V | NLDM Service File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the NLDM Service File.

INVOCATION: Exit gains control immediately prior to the output of records to the NLDM Service File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the NLDM Service File. This file is built from the SMF Type 39 Record (NLDM External Log Record), which can also be processed by the exit routine.

ELEMENTS AVAILABLE:

All elements in the NLDM Service File  
All elements in the SMF Type 39 Record

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

SPECIAL NOTE:

To implement this exit at the unit level, code it in prefix.MICS.USER.SOURCE(#SNTEXTIT).

SAMPLE USER EXIT:

In this sample exit, if the first three characters of the Performance Class name are not CIC, IMS, or TSO, then SKIP\_REC is set to ONE and the observation is deleted (that is, it is not written to the CA MICS database).

```
MACRO _USRSNSV
 PERFM = SUBSTR(NSVPCLSS,1,3);
 IF PERFM NE 'CIC' AND PERFM NE 'IMS' AND PERFM NE 'TSO'
 THEN SKIP_REC = ONE;
%
```

```
+-----+
| _ U S R S N V R | NetSpy Virtual Route Activity File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the CA NetSpy Virtual Route Activity File.

INVOCATION: Exit gains control immediately prior to the output of records to the CA NetSpy Virtual Route Activity File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the CA NetSpy Virtual Route Activity File. This file is built from the user-defined CA

NetSpy SMF record type.

#### ELEMENTS AVAILABLE:

All elements in the CA NetSpy Virtual Route Activity File  
All elements in the user-defined CA NetSpy SMF Record

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

#### SPECIAL NOTE:

To implement this exit at the unit level, code it in  
prefix.MICS.USER.SOURCE(#SNTEXTIT).

#### SAMPLE USER EXIT:

In this sample exit, the site has been collecting data about the activity and response times on multiple virtual routes to satisfy its real-time operational requirements, but it only wants to keep certain information in its CA MICS database. The USRSNVR exit is used to filter the information going into the CA MICS database to include only activity about the virtual routes to the host system (SYSA) that contains the production applications.

```
MACRO _USRSNVR
 IF SYSID NE 'SYSA' THEN SKIP_REC=ONE;
 %
+-----+
| _ U S R S P S U | NPM User Activity File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the NPM User Activity File.

INVOCATION: Exit gains control immediately prior to the output of records to the NPM User Activity File.

ACCOUNTING INTERFACE: This exit contains complex-level code and is used by the CA MICS Accounting and Chargeback Option. To use this file exit for user-specified modifications, see Section 4.3 of the System Modification Guide.

USES: This exit is used to add or change data elements, or to delete observations from the NPM User Activity File. This file is built from the NPM Session Statistics DETAIL Record, which can also be processed by the exit routine.

**ELEMENTS AVAILABLE:**

All elements in the NPM User Activity File  
All elements in the NPM Session Statistics DETAIL Record

**CODING RESTRICTIONS:** See the System Modification Guide, Section 4.3.

**SPECIAL NOTE:**

To implement this exit at the unit level, code it in  
prefix.MICS.USER.SOURCE(#SNTEXTIT).

**SAMPLE USER EXIT:**

In this sample exit, we want to retain certain critical terminal information to reduce the volume of observations in the database. If SLU is not a V52E008, V52E014, or V52E021 terminal, then SKIP\_REC is set to ONE and the observation is deleted (that is, it is not written to the CA MICS database).

**USER EXIT EXAMPLE #1:** CA MICS Accounting and Chargeback Option is not present in the database unit.

```
MACRO _USRSPSU
 IF SLU NE 'V52E008' AND SLU NE 'V52E014' AND
 SLU NE 'V52E021' THEN SKIP_REC = ONE;
%
```

**USER EXIT EXAMPLE #2:** CA MICS Accounting and Chargeback Option is present in the database unit.

Note that in this example, all deleted observations will pass through the accounting functions (calculations) prior to being deleted.

```
MACRO _USRSPSU
 _USRUPSU _USRUJPS
 IF SLU NE 'V52E008' AND SLU NE 'V52E014' AND
 SLU NE 'V52E021' THEN SKIP_REC = ONE;
%
```

```
+-----+
| _ U S R S P S Y | NPM System (PLU) Activity File Exit
+-----+
```

**DESCRIPTION:** This exit allows access to the data elements used to build the records in the NPM System (PLU) Activity File.

INVOCATION: Exit gains control immediately prior to the output of records to the NPM System Activity File in the #PSYDSUM routine.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the NPM System (PLU) Activity File. This file is built from the DETAIL timespan of the NPM User Activity File. Input record processing for the NPM Session Statistics DETAIL File can be performed in the \_USRSEL exit or the \_USRSPSU exit.

ELEMENTS AVAILABLE:

All elements in the NPM System (PLU) Activity File  
All elements in the NPM User Activity File

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

SPECIAL NOTE:

To implement this exit at the unit level, code it in prefix.MICS.USER.SOURCE(#SNTEXTIT).

SAMPLE USER EXIT:

In this sample exit, observations for application TAFAPL01 are not needed in the database and are deleted (that is, they are not written to the CA MICS database).

```
MACRO _USRSPSY
 IF PLU = 'TAFAPL01' THEN SKIP_REC = ONE;
 %
+-----+
| _ U S R S R T E | NLDM Route File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the NLDM Route (NVS RTE) File.

INVOCATION: Exit gains control immediately prior to the output of records to the NLDM Route (NVS RTE) File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the NLDM Route File. This file is built from the SMF Type 39 Record. Input record processing for the NLDM SMF Type 39 Record can be performed in the \_USRSEL exit or the \_USRSRTE exit.

ELEMENTS AVAILABLE:

All elements in the NLDM Route File  
All elements in the NLDM SMF Type 39 Record

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

SPECIAL NOTE:

To implement this exit at the unit level, code it in prefix.MICS.USER.SOURCE(#SNTEXTIT).

SAMPLE USER EXIT:

In this sample exit, observations for application TAFAPL01 are not needed in the database and are deleted (that is, they are not written to the CA MICS database).

```
MACRO _USRSRTE
 IF PLU = 'TAFAPL01' THEN SKIP_REC = ONE;
 %
+-----+
| _ U S R S R T M | NLDM Response Time File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the NLDM Response Time File.

INVOCATION: Exit gains control immediately prior to the output of records to the NLDM Response Time File.

USES: This exit is used to add or change data elements, or to delete observations from the NLDM Response Time File. This file is built from the SMF Type 39 Record. Input record processing for the NLDM SMF Type 39 Record can be performed in the \_USRSEL exit or the \_USRSRTM exit.

ELEMENTS AVAILABLE:

All elements in the NLDM Response Time File  
All elements in the NLDM SMF Type 39 Record

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

SPECIAL NOTES:

To implement this exit at the unit level, code it in prefix.MICS.USER.SOURCE(#SNTEXTIT).

ACCOUNTING INTERFACE: This exit contains complex-level code and is used by the CA MICS Accounting and Chargeback Option. To use this file exit for user-specified modifications, see Section 4.3 of the System Modification Guide.

SAMPLE USER EXIT:

In this sample exit, you want to retain certain critical terminal information to reduce the volume of observations in the database. If the number of responses for this observation during a session is less than five, the observation is deleted (that is, it is not written to the CA MICS database).

USER EXIT EXAMPLE #1: CA MICS Accounting and Chargeback Option is not present in the database unit.

```
MACRO _USRSRTM
 IF RTMTRESC LT 5 THEN SKIP_REC = ONE;
%
```

USER EXIT EXAMPLE #2: CA MICS Accounting and Chargeback Option is present in the database unit.

Note that in this example, all deleted observations will pass through the accounting functions (calculations) prior to being deleted.

```
MACRO _USRSRTM
 _USRRTM _USRJRT
 IF RTMTRESC LT 5 THEN SKIP_REC=ONE;
%
+-----+
| _ U S R S V B F | NLDM VTAM BIND Failure File Exit
+-----+
```

DESCRIPTION: This exit, as shipped by CA, contains code that eliminates certain records from the NLDM VTAM BIND Failure (NVSVBFB) File. It allows access to the data elements used to build the records in the NVSVBF file. To minimize the size of the NVSVBF file and to prevent it from containing

potentially useless information, the following UNBIND codes have been excluded.

| CODE | REASON                                                             |
|------|--------------------------------------------------------------------|
| ---- | -----                                                              |
| 01   | Normal session end                                                 |
| 02   | BIND forthcoming (normally issued by<br>a controlling application) |
| 0F   | Cleanup                                                            |
| 11   | Gateway node cleanup                                               |

The BIND Failure (BINDF) and Cross-domain Session Setup Failure (CDSESSSF) codes are not present in the NVSVPF file because the REQUEST-UNIT descriptions for BINDF and CDSESSSF have been dropped from IBM's documentation. The codes that correspond to BINDF and CDSESSSF are 80, 40, 20, and 10.

For additional information on the above codes, see IBM's SNA Reference Summary, which is an earlier version of IBM guide GA27-3136 (for example, -6).

If you want to keep these records in your data center's database, remove the code that deletes the BIND failure codes and selected UNBIND codes from prefix.MICS.SOURCE(#SNTEXIT).

INVOCATION: Exit gains control immediately prior to the output of observations to the NLDM VTAM BIND Failure File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the NLDM VTAM BIND Failure File. This file is built from the SMF type 39 record. Input record processing for the NLDM SMF type 39 record can be performed in the \_USRSEL exit.

#### ELEMENTS AVAILABLE:

All elements in the NLDM VTAM BIND Failure File  
All elements in the NLDM SMF Type 39 Record

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

SPECIAL NOTES:



1. To implement this exit at the unit level, code it in `prefix.MICS.USER.SOURCE(#SNTEXTIT)`.
2. As described above, this exit is shipped with SAS code that eliminates certain failure codes from the MVSVBFB file. If you want to retain one or more of these codes in your data center's database, we recommend that you recode the logic to delete observations in the prefix-level USER.SOURCE library.

#### SAMPLE USER EXIT:

In this sample exit, observations for terminals attached to control unit (SLUPU) T01CU003 are deleted.

```
MACRO _USRSVBF
 IF SLUPU = 'T01CU003' THEN SKIP_REC = ONE;
 %
+-----+
| _ U S R X C A F | SNTCAF DETAIL TimeSpan File Exit
+-----+
```

**DESCRIPTION:** This exit allows the SNTCAF file to be built at the DETAIL timespan. By default, the SNTCAF file is not supported at the DETAIL timespan.

**INVOCATION:** Exit gains control immediately prior to the data step in `sharedprefix.MICS.SOURCE(#CAFDSUM)` that builds the DAYS timespan SNTCAF file.

**ACCOUNTING INTERFACE:** No interface to CA MICS Accounting and Chargeback Option.

**USES:** While the SNTCAF file is not supported by default in the DETAIL timespan, some sites must create it in this timespan. The \_USRXCFAF exit provides this capability.

#### ELEMENTS AVAILABLE:

All elements in the NPM components Activity File (SNTCAF)

**CODING RESTRICTIONS:** See the System Modification Guide, Section 4.3.

#### SPECIAL NOTE:

To implement this exit at the unit level, code it in `prefix.MICS.USER.SOURCE(#SNTEXTIT)`.

**SAMPLE USER EXIT:**

In this sample exit, the site will build a single SNTCAF01 file in the DETAIL timespan.

```
MACRO _USRXCAF
 DATA &SNTX..SNTCAF01 (%%CAFFILE(OP=FILEOPTS,TS=DETAIL)
 LABEL='NPM COMPONENTS ACTIVITY FILE');
 %%CAFFMT(TS=DETAIL);
 %%CAFLEN(TS=DETAIL,TYPE=BOTH);
 %%CAFLBL;
 SET WORK.SNTCAF00;
 %%CAFDERV;
 RUN;
%
```

```
+-----+
| _ U S R S N A C | NCP Network Accounting File Exit
+-----+
```

**DESCRIPTION:** This exit allows access to the data elements used to build the records in the NCP Network Accounting File.

**INVOCATION:** Exit gains control immediately prior to the output of records to the NCP Network Accounting File.

**ACCOUNTING INTERFACE:** This exit contains complex-level code and is used by the CA MICS Accounting and Chargeback Option. To use this file exit for user-specified modifications, see Section 4.3 of the System Modification Guide.

**USES:** This exit is used to add or change data elements, or to delete observations from the NCP Network Accounting File. This file is built from either the CA NetSpy SMF network session accounting/network gateway accounting subtype C records (SMF record number is user-defined) or the NPM SMF type 28 network session accounting/network gateway accounting records, all of which can be processed by this exit routine.

**ELEMENTS AVAILABLE:**

All elements in the NCP Network Accounting File  
All elements in the CA NetSpy or NPM SMF records listed under 'USES' above.

**CODING RESTRICTIONS:** See the System Modification Guide, Section 4.3.

**SPECIAL NOTE:**

To implement this exit at the unit level, code it in  
prefix.MICS.USER.SOURCE(#SNTEXTIT).

#### SAMPLE USER EXIT:

In this sample exit, we want to drop all CA NetSpy network session accounting records that were collected for the PLU side of the session. We are doing this to eliminate duplicate network session accounting data: we had tailored CA NetSpy to collect data on both sides (PLU and SLU) of the same session. If the Data Collection Point (NACCOLPT) for the observation is not SLU, then SKIP\_REC is set to ONE and the observation is deleted (that is, it is not written to the CA MICS database).

The CA MICS Accounting and Chargeback Option is not present in the database unit.

```
MACRO _USRSNAC
 IF NACCOLPT NE 'SLU' THEN SKIP_REC = ONE;
 %
+-----+
| _ U S R S L N F | NPDA LAN File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the NPDA LAN File.

INVOCATION: Exit gains control immediately prior to the output of records to the NPDA LAN File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the LAN File. This file is built from the NetView Hardware Monitor SMF Type 37 Records.

#### ELEMENTS AVAILABLE:

All elements in the NPDA LAN File

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

#### SPECIAL NOTE:

To implement this exit at the unit level, code it in

```
prefix.MICS.USER.SOURCE(#SNTEXTIT).
```

**SAMPLE USER EXIT:**

In this sample exit, a check is performed to determine if the NPDA General Event Cause Code is undefined (for example, equal to 'FF'). If so, SKIP\_REC is set to ONE and the observation is deleted (that is, it is not written to the CA MICS database).

```
MACRO _USRSLNF
 IF SNTGEVCC = 'FF' THEN SKIP_REC = ONE;
%
```

```
+-----+
| _ U S R S G A F | NPDA Generic Alert File Exit
+-----+
```

**DESCRIPTION:** This exit allows access to the data elements used to build the records in the NPDA Generic Alert File.

**INVOCATION:** Exit gains control immediately prior to the output of records to the NPDA Generic Alert File.

**ACCOUNTING INTERFACE:** No interface to CA MICS Accounting and Chargeback Option.

**USES:** This exit is used to add or change data elements, or to delete observations from the NPDA Generic Alert File. This file is built from the NetView Hardware Monitor SMF Type 37 Records.

**ELEMENTS AVAILABLE:**

All elements in the NPDA Generic Alert File

**CODING RESTRICTIONS:** See the System Modification Guide, Section 4.3.

**SPECIAL NOTE:**

To implement this exit at the unit level, code it in  
prefix.MICS.USER.SOURCE(#SNTEXTIT).

**SAMPLE USER EXIT:**

In this exit, if the failing resource name is CHCAU1, then SKIP\_REC is set to ONE and the observation is deleted (that is, it is not written to the CA MICS database).

```
MACRO _USRSGAF
 IF SNTFRNAM = 'CHCAU1' THEN SKIP_REC = ONE;
%
```

```
+-----+
| _ U S R S V B S | VTAM Buffer Data File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the VTAM Buffer Data File.

INVOCATION: Exit gains control immediately prior to the output of records to the VTAM Buffer Data File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the VTAM Buffer Data File. This file is built from the NetView Performance Monitor SMF type 28 records.

ELEMENTS AVAILABLE:

All elements in the VTAM Buffer Data File.

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

SPECIAL NOTE:

To implement this exit at the unit level, code it in prefix.MICS.USER.SOURCE(#SNTEXTIT).

SAMPLE USER EXIT:

In this exit, if the data is from non-prime shift, then SKIP\_REC is set to ONE and the observation is deleted (that is, it is not written to the CA MICS database).

```
MACRO _USRSVBS
 IF ZONE NE 2 THEN SKIP_REC = ONE;
%
```

```
+-----+
| _ U S R S V C S | VTAM CSM Data File Exit
+-----+
```

**DESCRIPTION:** This exit allows access to the data elements used to build the records in the VTAM Communication Storage File.

**INVOCATION:** Exit gains control immediately prior to the output of records to the VTAM Communication Storage File.

**ACCOUNTING INTERFACE:** No interface to CA MICS Accounting and Chargeback Option.

**USES:** This exit is used to add or change data elements, or to delete observations from the VTAM Communication Storage File. This file is built from the NetView Performance Monitor SMF type 28 records.

**ELEMENTS AVAILABLE:**

All elements in the VTAM Communication Storage File.

**CODING RESTRICTIONS:** See the System Modification Guide, Section 4.3.

**SPECIAL NOTE:**

To implement this exit at the unit level, code it in prefix.MICS.USER.SOURCE(#SNTEXTIT).

**SAMPLE USER EXIT:**

In this exit, if the data is from STORAGE type, then SKIP\_REC is set to ONE and the observation is deleted (that is, it is not written to the CA MICS database).

```
MACRO _USRSVCS
 IF VCSVDTYP = 'STORAGE' THEN SKIP_REC = ONE;
%
```

```
+-----+
| _ U S R S V G B | VTAM Global Data File Exit
+-----+
```

**DESCRIPTION:** This exit allows access to the data elements used to build the records in the VTAM Global Data File.

**INVOCATION:** Exit gains control immediately prior to the output of records to the VTAM Global Data File.

**ACCOUNTING INTERFACE:** No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the VTAM Global Data File. This file is built from the NetView Performance Monitor SMF type 28 records.

ELEMENTS AVAILABLE:

All elements in the VTAM Global Data File.

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

SPECIAL NOTE:

To implement this exit at the unit level, code it in prefix.MICS.USER.SOURCE(#SNTEXTIT).

SAMPLE USER EXIT:

In this exit, if the VTAM tuning statistics task record is displayed at console, then SKIP\_REC is set to ONE and the observation is deleted (that is, it is not written to the CA MICS database).

```
MACRO _USRSVGB
 IF VGBTNSTA = '...1....' THEN SKIP_REC = ONE;
%
```

```
+-----+
| U S R S N T S | Telnet Server Entry File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the Telnet Server Entry File.

INVOCATION: Exit gains control immediately prior to the output of records to the Telnet Server Entry File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the Telnet Server Entry File. This file is built from the CA NetSpy SMF records.

ELEMENTS AVAILABLE:

All elements in the Telnet Server Entry File

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

```
+-----+
| U S R S S T N | Telnet Server File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the Telnet Server File.

INVOCATION: Exit gains control immediately prior to the output of records to the Telnet Server File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the Telnet Server File. This file is built from the TCP/IP for z/OS SMF Type 118 records with a value of 'LOGN' or 'LOGF' at offset 21.

ELEMENTS AVAILABLE:

All elements in the Telnet Server File

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

```
+-----+
| U S R S C T N | Telnet Client File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the Telnet Client File.

INVOCATION: Exit gains control immediately prior to the output of records to the Telnet Client File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the Telnet Client File. This file is built from the TCP/IP for z/OS SMF Type 118 records with a value of 'LGON' or 'LGOF' at offset 21.

ELEMENTS AVAILABLE:



All elements in the Telnet Client File

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

```
+-----+
| U S R S F S F | FTP Server File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the FTP Server File.

INVOCATION: Exit gains control immediately prior to the output of records to the FTP Server File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the FTP Server File. This file is built from the TCP/IP for z/OS SMF Type 118 records, a four-character FTP command at offset 21, and a value of 'S' at offset 69.

ELEMENTS AVAILABLE:

All elements in the FTP Server File

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

```
+-----+
| U S R S F C F | FTP Client File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the FTP Client File.

INVOCATION: Exit gains control immediately prior to the output of records to the FTP Client File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the FTP Client File. This file is built from the TCP/IP for z/OS SMF Type 118 records, a four-character FTP command at offset 21, and a value of 'C' at offset 69.

### ELEMENTS AVAILABLE:

All elements in the FTP Client File

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

```
+-----+
| U S R S A P I | API Calls for Sockets File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the API Calls for Sockets File.

INVOCATION: Exit gains control immediately prior to the output of records to the API Calls for Sockets File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the API Calls for Sockets File. This file is built from the TCP/IP for z/OS SMF Type 118 records with a value of 'INIT' or 'TERM' at offset 21.

### ELEMENTS AVAILABLE:

All elements in the API Calls for Sockets File.

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

```
+-----+
| U S R S F L F | FTP Login Failure File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the FTP Login Failure File.

INVOCATION: Exit gains control immediately prior to the output of records to the FTP Login Failure File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the FTP Login Failure File. This

file is built from the SMF Type 119 subtype 72 records.

ELEMENTS AVAILABLE:

All elements in the FTP Login Failure File.

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

```
+-----+
| U S R S I P X | IP Protocol Statistics File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the IP Protocol Statistics File.

INVOCATION: Exit gains control immediately prior to the output of records to the IP Protocol Statistics File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the IP Protocol Statistics File. This file is built from the SMF Type 119 subtype 5 records.

ELEMENTS AVAILABLE:

All elements in the IP Protocol Statistics File.

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

```
+-----+
| U S R S I C X | ICMP Protocol Statistics File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the ICMP Protocol Statistics File.

INVOCATION: Exit gains control immediately prior to the output of records to the ICMP Protocol Statistics File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the ICMP Protocol Statistics

File. This file is built from the SMF Type 119 subtype 5 records.

ELEMENTS AVAILABLE:

All elements in the ICMP Protocol Statistics File.

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

```
+-----+
| U S R S T C I | TCP Protocol Statistics File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the TCP Protocol Statistics File.

INVOCATION: Exit gains control immediately prior to the output of records to the TCP Protocol Statistics File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the TCP Protocol Statistics File. This file is built from the SMF Type 119 subtype 5 records.

ELEMENTS AVAILABLE:

All elements in the TCP Protocol Statistics File.

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

```
+-----+
| U S R S U D I | UDP Protocol Statistics File Exit
+-----+
```

DESCRIPTION: This exit allows access to the data elements used to build the records in the UDP Protocol Statistics File.

INVOCATION: Exit gains control immediately prior to the output of records to the UDP Protocol Statistics File.

ACCOUNTING INTERFACE: No interface to CA MICS Accounting and Chargeback Option.

USES: This exit is used to add or change data elements, or to delete observations from the UDP Protocol Statistics File. This file is built from the SMF Type 119 subtype 5 records.

ELEMENTS AVAILABLE:

All elements in the UDP Protocol Statistics File.

CODING RESTRICTIONS: See the System Modification Guide, Section 4.3.

```
+-----+
| U S R T f f f | DETAIL Tape Data Selection Exit
+-----+
```

DESCRIPTION: The USRTfff exits provide access to DETAIL file records prior to their output to DETAIL tape data sets. Refer to Chapter 7 of this guide for information about DETAIL tape processing and a list of eligible component files.

INVOCATION: The USRTfff exit is invoked prior to output to DETAIL tape files.

ACCOUNTING INTERFACE: No interface is provided.

USES: Use this exit to limit the amount of data that is written to DETAIL tape files, or to modify the contents of data elements written to DETAIL tape files. Note that USRTfff exit code only affects the DETAIL tape file content for a particular file (fff). It has no impact on the normal unit database content for the same file (fff).

ELEMENTS AVAILABLE: All elements in the DETAIL timespan of the file.

ACTIVATION: The USRTfff exits are invoked using the indirect exit convention described in section 4.3.1.2 of the System Modification Guide. See this section for a detailed discussion of indirect exit coding.

All of the USRTfff indirect exits are activated in sharedprefix.MICS.SOURCE(#SNTEXIT). In #SNTEXIT, you will find the following statement for each file (fff) eligible for DETAIL tape:

```
%LET USRTfff = ;
```

The exit is activated by providing a member name to the right of the equal sign:

```
%LET USRTfff = exitname ;
```

If you code an exitname, you MUST create a member in each unit's prefix.MICS.USER.SOURCE library with that name. Provide valid SAS code in the member. This code will be invoked prior to the output of records to the DETAIL tape file.

Example:

```
sharedprefix.MICS.SOURCE(#SNTEXTIT):
```

```
%LET USRTAPI = APITEXIT ;
```

```
prefix.MICS.USER.SOURCE(APITEXIT):
```

```
IF APIBYTEI = 0 AND APIBYTE0 = 0 THEN SKIP_REC=1 ;
```

In this example, APITEXIT was chosen as the name for the DETAIL tape exit for the TCPAPI file. Member APITEXIT was created in the unit level prefix.MICS.USER.SOURCE library for each unit where DETAIL tape was activated for the TCPAPI file.

The exit was coded to limit the observation written to the DETAIL tape file to those where APIBYTEI and APIBYTE0 contained positive non-zero values.

Note that the exit member name must be identical in each unit's prefix.MICS.USER.SOURCE library, but the contents of each member can be different (or identical) for each unit.

**CODING RESTRICTIONS:** Ensure that you have activated DETAIL tape processing for a file, and executed SNTPGEN prior to activating and coding USRTfff exits.

## 10.5 Implement Incremental Update

If you are using the TAPEfff option or USRXfff exits to collect detail level data, and incremental update is active, you may need to make a few simple but very important adjustments to your exits or options to accommodate the way that incremental update processes data.

This section discusses the following:

- o TAPEfff option considerations with incremental update
- o USRXfff exit considerations with incremental update
  - DETAIL tape files created in USRXfff exits
  - DASD files created in USRXfff exits

### TAPEfff OPTION CONSIDERATIONS WITH INCREMENTAL UPDATE

The TAPEfff option allows the creation of DETAIL timespan tape files for certain high volume files.

Without incremental update, a single DETAIL timespan tape file is created for TAPEfff activated files during the DAILY run. The general practice is to use GDGs so that the (+0) tape volume contains yesterday's data, (-1) contains the prior day's data, and so on.

With incremental update activated, a tape is created with each execution of an incremental update as well as a final tape during the DAILY update run. For example, three incremental updates followed by a final daily update run result in a total of four tapes created, one for each TAPEfff activated file. Each tape contains only the detail data encountered during the individual incremental update or daily run. If you are employing GDGs you will want to consider increasing the number of generations to encompass the desired time range of history. For example, if previously 7 "daily" generations were maintained and you run 4 increments per day, you may wish to expand the generations kept to 28 (7 times 4 updates per day).

The use of fewer tapes in a single update under the incremental feature expedites processing. In addition, due to the "special study" nature of the data, separation into multiple pieces representing period time slices should allow usage to be more direct. That is, the data is already subset to the period contained within the update.

You also may consider creating a standalone job to consolidate these individual tapes into a single one after

the DAILY job completes if you prefer to have a single tape data set contain all transactions for the time range.

### USRXfff EXIT CONSIDERATIONS WITH INCREMENTAL UPDATE

The USRXfff exits allow client supplied code to force the creation of SAS files containing DETAIL level data. These exits were provided for specific high volume transaction based data that are populated at the DAYS and higher timespans in a summarized form in CA MICS. Due to the high volume of data involved, these exits may be used to create tape files, although nothing other than space considerations precludes creation of files on DASD with these exits.

Many of the products that provide USRXfff exits have implemented standardized approaches to collect DETAIL level data, thus removing the need for USRXfff exit coding. Any user code employed in USRXfff exits should be examined to ensure that the data and the approach are still required. Generally, transaction data at this level is employed for specific tuning projects or special studies centered on subsystem or application related issues and is needed only for occasional and isolated time periods.

If you are using incremental update and find that the USRXfff exits you have coded are still required for your operation, be sure to review the considerations below.

### DETAIL TAPE FILES CREATED IN USRXfff EXITS

When using the exits to write to tape without incremental update activated, a single tape file is created from the user written code in each activated USRXfff exit. The general practice is to use generation data groups (GDGs) to retain history. In this case, it is assumed that CA MICS units are updated once a day with yesterday's data. Without incremental update the generation 0 (+0) tape data set would contain data from the previous CA MICS update (yesterday), (-1) contains the prior run (two days ago), and so on.

With incremental update, a tape file is again created from the user written code in each activated USRXfff exit with each execution of an update. However, rather than running CA MICS updates once per day, incremental update implies multiple update runs daily. For example, three



incremental updates followed by a final daily update run result in a total of four tapes in one day, one created from each activated USRXfff exit. Each tape contains only the detail data encountered during the individual incremental update or daily run. If you are employing GDGs you will want to evaluate increasing the number of generations to encompass the desired time range of history. For example, if previously 7 "daily" generations were maintained and you ran 4 increments per day, you may wish to expand the generations kept to 28 (7 times 4 updates per day).

The use of fewer tapes in a single update under the incremental feature expedites processing. In addition, in keeping with the "special study" nature of the data, separation of the data into multiple pieces representing the narrower period slices should simplify usage. That is, the data is already subset to the period contained within the update.

You also may consider creating a standalone job to consolidate these individual tapes into a single one after the DAILY job completes if you prefer to have a single tape data set contain all transactions for the time range.

#### DASD FILES CREATED IN USRXfff EXITS

Either of two basic approaches may be employed when using the exits to write to DASD files. Data can be written to detail data set(s) of CA MICS units. Or it can be written to data sets allocated externally to the CA MICS units (such as a user data set that has been added to the Daily JCL stream). In either scenario the SAS file written by the exit will be replaced by new data with each execution of the update step.

If the exit is writing to the CA MICS Detail data set and the recommended approach has been taken with the exit then no change to outputs will occur under incremental update. The recommended approach employs indirect coding to reference the database (uses "&iit" not "DETAIL" in the data step) and an active detail status (file status of "Y" at the detail timespan in cccGENIN and cccCGEN has been executed). When these conditions are in place the file created by the exit will be treated as other CA MICS files in incremental update mode and at the conclusion of the Daily job stream a single file containing data from all increments will be available in the detail unit

database. If the file status is not active, only data from the last incremental execution will be present.

An alternative to selective exit coding is to employ a generation data set (GDG) structure for the external DASD file. In this scenario GDG entries to cover the incremental updates would be defined and each incremental run would write to a new GDG entry which would contain data for the increment. Each series of incremental runs followed by a DAILY job execution would create a new series of GDG data sets. While this approach allows you to capture all data on an ongoing basis, use of the unit detail data set as described above is more efficient and is the recommended approach.

# Appendix A: Messages

---

## Messages

### SNT00102

```
+-----+
| S N T 0 0 1 0 2 |
+-----+
```

TEXT: NO DATA SOURCES SPECIFIED IN SNTOPS. THIS MAY  
CAUSE USER 300 ABEND.

TYPE: Warning

REASON: There are no data source parameters coded on the  
DATA SOURCES statement contained in  
prefix.MICS.PARMS(SNTOPS). CA MICS keeps only  
records that pertain to the data sources  
specified on this keyword parameter. This  
message is issued as a warning that failure to  
code at least one data source may cause CA MICS  
to abend.

ACTION: Code one or more of the following parameters on  
the DATA SOURCES keyword parameter  
prefix.MICS.PARMS(SNTOPS):

NPMN, NPMS, NLDM, NPDA, NSPY, NTS, or NEWS.

REFERENCES: Section 7.3.1, Processing Options (SNTOPS)

## SNT00103

```
+-----+
| S N T 0 0 1 0 3 |
+-----+
```

TEXT: TOTAL SNT TYPE RECORDS FROM INPUT

```

NPM SMF 28 = %ISMF28
NPDA SMF 37 = %ISMF37
NLDM SMF 39 = %ISMF39
NSPY/NTCP RECS = %INSPY
TCP SMF %SMF118 = %I118
TCP SMF %SMF119 = %I119

```

TOTAL = %TISMF

TYPE: Information

REASON: This message is issued to provide runtime control counts. The numbers represent the number of records read from the INPUTSMF file for each data source.

ACTION: None

REFERENCES: None

**SNT00104**

```
+-----+
| S N T 0 0 1 0 4 |
+-----+
```

TEXT: TOTAL SNT TYPE RECORDS KEPT

```
NPM SMF28 NTWK = %KSMF28N
NPM SMF28 SESS = %KSMF28S
NPM SMF28 VTAM = %KSMF28V
NPDA SMF 37 = %KSMF37
NLDM SMF 39 = %KSMF39
NSPY/NTCP RECS = %KNSPY
TCP SMF %SMF118 = %K118
TCP SMF %SMF119 = %K119
```

```

TOTAL = %TKSMF
```

TYPE: Information

REASON: This message is issued to provide runtime control counts. The numbers represent the number of records kept from the INPUTSMF file for each data source.

ACTION: None

REFERENCES: None

## SNT00105

```
+-----+
| S N T 0 0 1 0 5 |
+-----+
```

TEXT: RECORD SUMMARY STATISTICS

```
TOTAL INPUT RECORDS READ = %INSMF
TOTAL NON-SNT RECORDS DROPPED = %NONSNT
TOTAL SNT TYPE RECORDS READ = %TISMF
TOTAL SNT TYPE RECORDS DELETED = %SNTDEL
TOTAL SNT TYPE RECORDS KEPT = %TKSMF
```

%CTPCT %P OF ALL RECORDS READ WERE SNT TYPES.

%CKPCTI %P OF ALL SNT TYPE RECORDS READ WERE KEPT.

%CKPCTT %P OF ALL RECORDS READ WERE KEPT.

END OF RECORD SUMMARY STATISTICS

TYPE: Information

REASON: This message provides runtime control counts. The numbers represent the total number of records read, the percent of the records that were related to the CA MICS Network Analyzer, the percent of CA MICS Network Analyzer records that were kept, and the percent of all records that were kept.

ACTION: None

REFERENCES: None

**SNT00106**

```
+-----+
| S N T 0 0 1 0 6 |
+-----+
```

TEXT:           OBSERVATIONS SKIPPED BY USER EXITS IN THE MAIN  
                  DATA STEP

```
USRSNEF = %NEFEXIT
USRSNSF = %NSFEXIT
USRSNAF = %NAFEXIT
USRSNCL = %NCLEXIT
USRSNNW = %NNWEXIT
USRSNIN = %NINEXIT
USRSNVR = %NSSEXIT
USRSGAF = %GAFEXIT
USRSLNF = %LNFEXIT
USRSCAF = %CAFEXIT
USRSTCP = %TCPEXIT
USRSVBS = %VBSEXIT
USRSVCS = %VCSEXIT
USRSVGB = %VGBEXIT

TOTAL = %TOTEXIT
```

TYPE:           Information

REASON:          This message is issued to provide runtime  
                  control counts of the number of observations  
                  that were deleted by each of the indicated file  
                  exits in the main DATA step.

ACTION:          None

REFERENCES:      Section 9.2 of this guide

## SNT00107

```
+-----+
| S N T 0 0 1 0 7 |
+-----+
```

TEXT:           INVALID RECORD SUBTYPE FOUND FOR: %USESSIDC .  
                  SUB TYPE FOUND = %NLDRSUBT .

TYPE:           Warning

REASON:          The value of the session mask data element is  
                  based on the NetView SMF Type 39 Record Subtype,  
                  which must have a value of between one and six.  
                  This message is issued if the NetView SMF Type  
                  39 Record subtype has a value other than one  
                  through six. This may indicate that a new  
                  version of NetView is in use or an erroneous  
                  record has been generated by NetView or by the  
                  program that creates the input file for the CA  
                  MICS Network Analyzer.

ACTION:          For assistance, contact Technical Support at  
                  <http://ca.com/support>.

REFERENCES:      None



**SNT00108**

```
+-----+
| S N T 0 0 1 0 8 |
+-----+
```

TEXT:       OBSERVATIONS SKIPPED BY USER EXIT IN ROUTINE  
             %ROUTINE

             %EXIT = %EXITCNT'

TYPE:       Information

REASON:     This message is issued by one of the #fffdSUM  
             routines if you use the #USRsfff exit to delete  
             an observation. The message indicates which  
             routines produced the message and the file in  
             which the deletion occurred (for example,  
             #fffdSUM, where fff is CAF, LSY, NCA, NLL,  
             NPL, NSC, or PSY).

ACTION:     None

REFERENCES:  None

## SNT00109

```
+-----+
| S N T 0 0 1 0 9 |
+-----+
```

TEXT:           OBSERVATIONS SKIPPED BY USER EXITS IN THE SECOND  
                  DATA STEP

```
USRSNSA = %NSAEXIT
USRSNSV = %NSVEXIT
USRSRTE = %RTEEXIT
USRSRTM = %RTMEXIT
USRSVBF = %VBFEXIT
USRSNLW = %NLWEXIT
USRSNSC = %NSCEXIT
```

```

TOTAL = %TOTEXIT
```

TYPE:           Information

REASON:          This message is issued as a runtime control that  
                  informs you of the number of observations  
                  deleted by each of the indicated file exits in  
                  the second DATA step.

ACTION:          None

REFERENCES:      Section 9.2 of this guide

**SNT00138**

```
+-----+
| S N T 0 0 1 3 8 |
+-----+
```

TEXT: NETSPY TYPE U RECORDS DROPPED: %DRPUCNTR

TYPE: Information

REASON: CA NetSpy has the ability to create two SMF record types that contain essentially the same information. The CA MICS Network Analyzer will delete the subtype U records when they are found with the subtype S records. This message reports the number of U records deleted.

ACTION: None

REFERENCES: Chapter 6 of this guide

## SNT00139

```
+-----+
| S N T 0 0 1 3 9 |
+-----+
```

TEXT:           SESSION MANAGER OBSERVATIONS DROPPED: %NSSMGR

TYPE:           Information

REASON:        CA NetSpy has the ability to interface directly with certain vendors' session manager software. This interface allows CA NetSpy to maintain the integrity of some data elements that would otherwise be rendered useless. A byproduct of this interface is that CA NetSpy will create more than one record for each terminal in session with the session manager. The CA MICS Network Analyzer offers the ability to delete the observations that contain data relating to the session between the terminal and the session manager, thus keeping only the data relating to the terminal and the application or applications it is actually in session with.

This message tells you how many of the session manager observations were actually deleted. The message will not appear if no observations were deleted.

ACTION:        None

REFERENCES:    Chapter 6 of this guide

**SNT00140**

```
+-----+
| S N T 0 0 1 4 0 |
+-----+
```

TEXT: RECORDS RESET BECAUSE TOTAL RESPONSE COUNT WAS LESS THAN THE SUM OF RESPONSE DISTRIBUTIONS 1 THROUGH 4. RESPONSE DISTRIBUTION COUNTER 5 WAS SET TO ZERO IN THESE OBSERVATIONS.  
NUMBER RESET: %NSPYBADD FROM FILE %NSFILEID

TYPE: Information

REASON: The last response distribution counter (5) typically contains the number of responses that exceeded the last response target specified to CA NetSpy. The value of this field is derived by subtracting the sum of the four response distribution counters from the total response counter.

Under certain normal circumstances, CA NetSpy's response distribution counters total exceeds the field that contains the total number of responses. When this happens, the last counter value contains a negative number. In this case, the value is reset to zero.

ACTION: None

REFERENCES: None

## SNT00141

```
+-----+
| S N T 0 0 1 4 1 |
+-----+
```

TEXT: MISMATCH OCCURRED MATCHING NSP AND NSS FILES.  
OBS ON NSS FILE HAD NO MATCH ON NSP FILE DURING  
MERGE. NUMBER OF MISMATCHES: %NUMBER  
or  
MISMATCH OCCURRED MATCHING NSP AND NSS FILES.  
OBS ON NSP FILE HAD NO MATCH ON NSS FILE DURING  
MERGE. NUMBER OF MISMATCHES: %NUMBER

TYPE: Information

REASON: The NSP and NSS files must be matched (MERGED)  
in order to pass critical variables from the NSP  
into the NSS file.

This message indicates that there was no match  
for one or more observations. The message is  
printed only once at the end of the DATA step,  
and prints out the total number of mismatches.

A mismatch will occur in either of two cases:

1. An observation is found for an application  
but there is no corresponding observation  
for a terminal associated with that  
application.
2. An observation is found for a terminal, but  
there is no corresponding observation for an  
application associated with that terminal.

The first case occurs when the CA NetSpy  
monitors an application during an interval in  
which no terminal is logged on to the  
application. The second case occurs when a  
terminal is logged on (through a multiple  
session manager application) to an application  
that CA NetSpy is not monitoring.

ACTION: No action is needed in the first case discussed  
above. In the second case, one should activate  
CA NetSpy monitoring of the application that is  
being accessed through the multiple session  
manager in order to retain observations for

terminal sessions with that application.

REFERENCES: None

## SNT00142

```
+-----+
| S N T 0 0 1 4 2 |
+-----+
```

TEXT: AN INVALID CONDITION OCCURRED DURING PROCESSING  
%MSGCOND

where MSGCOND may be one of the following:

- 1) INVALID SMF 38 SUB TYPE FOUND IN SNTNET3
- 2) INVALID SMF 28 SUB TYPE FOUND IN SNTNET3
- 3) INVALID SMF 28 SUB TYPE FOUND IN SNTNPS3
- 4) INVALID SMF RECORD FOUND IN SNTNET3
- 5) INVALID SMF RECORD FOUND IN SNTNPS3
- 6) SMF 28 RCD SESSION DATA OFFSETS INCORRECT
- 7) INVALID TIME STAMP FOUND IN SNTNLD4

TYPE: Warning

REASON: Messages 1, 2, and 3: Only certain NPM record subtypes are used for processing both the old SMF 38 records and the newer SMF 28 records. Under normal circumstances, the unnecessary subtypes are filtered or dropped as soon as they are recognized in the daily job. These messages appear if an incorrect subtype is found after it should have been dropped.

Messages 4 and 5 appear if an incorrect SMF record number is found in module SNTNET3 or SNTNPS3 after the filtering process.

Message 6 appears if the proper SMF 28 data sessions are not available.

Message 7 appears if an invalid timestamp is found in module SNTNLD4 while processing NetView Session Monitor or CA NetMaster SMF 39 records.

ACTION: None of the above messages should normally occur. If they do, CA MICS network processing must have encountered an invalid input record and deleted it. If you receive many of these messages, or you suspect that there are serious errors in your input data, contact CA Technical Support at <http://ca.com/support>.

REFERENCES: None



**SNT00143**

```
+-----+
| S N T 0 0 1 4 3 |
+-----+
```

TEXT: Variable

TYPE: Information

REASON: After all input records are read in the DAILY job, this message is used to produce a report in the MICSL0G outlining the data read in the job. For each SMF record type the report lists each subtype read, the data source, and the low and high SMF timestamp.

ACTION: This report can be very useful in determining if the proper data is being read into the DAILY job.

REFERENCES: None

## SNT00144

```
+-----+
| S N T 0 0 1 4 4 |
+-----+
```

TEXT: SMF TYPE 39 INVALID DATE CONDITION FOUND  
 %DATELINE  
 INPUT RECORD NUMBER: %\_N\_  
 SMF END TIME STAMP : %CHAR\_TS

where DATELINE may be one of the below:

- 1) RTM START TIME STAMP GT END TIME STAMP
- 2) RTM START TIME STAMP LE ZERO
- 3) RTMENDTS GT CURRENT DATE/TIME
- 4) RTMENDTS LE ZERO
- 5) ACT START TIME STAMP GT END TIME STAMP
- 6) ACT START TIME STAMP LE ZERO
- 7) ACTENDTS GT CURRENT DATE/TIME
- 8) ACTENDTS LE ZERO

where \_N\_ is the input (relative) record number.

where CHAR\_TS is the SMF timestamp of the input record causing the message to appear.

TYPE: Warning

REASON: There appears to be some problems with the timestamp fields in the Accounting and Availability data section of the SMF type 39 records. To date, we have seen the start timestamp equal to zero in some records, and greater than the end timestamp in other records. These incorrect timestamps have been found in both Tivoli Netview and CA NetMaster versions of the type 39 record.

There have not been any incorrect date problems found in the RTM data section, but the date checks were added there for safety.

The message text, specifically the DATELINE value above, explains the condition found.

ACTION: In cases 1, 2, 5, and 6 above, the CA MICS Network Analyzer will reset the start timestamp equal to the end timestamp for the appropriate data section (RTM or ACT). For cases 3, 4, 7,

and 8 above, the end timestamp will be set equal to the current timestamp minus one day, in an attempt to put the record close to what would normally be the previous day's input time range.

It is recommended that the appropriate vendor (Tivoli for Netview or CA for CA NetMaster) be contacted regarding this problem. The message text will help you isolate the records having the problems.

REFERENCES: None

## SNT00145

```
+-----+
| S N T 0 0 1 4 5 |
+-----+
```

TEXT           %BAD\_STYP UNKNOWN RECORD SUBTYPES IN THE SMF  
TYPE 39 RECORDS HAVE BEEN DROPPED.'

where BAD\_STYP is the number of invalid Session Type records found and dropped from any further processing. Valid values for Session Type are:

1=LU-LU  
2=SSCP-LU  
3=SSCP-PU  
4=SSCP-SSCP

TYPE:          Warning

REASON:        Only 1 through 4 session type values are processed in CA MICS. Any value other than 1 through 4 is considered a bad session type. Hence the record is dropped from further DAILY processing.

ACTION:        The above message should not occur normally. If you receive many of these messages, or if you suspect there are serious errors in your input data, contact CA Technical Support at <http://ca.com/support>.

REFERENCES: None

## SNT00146

```
+-----+
| S N T 0 0 1 4 6 |
+-----+
```

TEXT: TCP/IP DATA SOURCE REQUESTED VIA SNTPGEN AND  
HERE WAS NO SMF RECORD TYPE SPECIFIED ON  
COMPTDEF OR A JCLGEN WAS NOT RUN (TO UPDATE  
prefix.MICS.PARMS(DBCONFIG) ).

TYPE: Termination

REASON: When the TCP/IP data source is specified, you  
must specify the SMF record type on:

sharedprefix.MICS.GENLIB(COMPTDEF)

ACTION: The TCP/IP SMF record type is the sixth number  
on the SNT statement. If it is present on  
COMPTDEF, the probable cause is that a JCLGEN  
must be run. JCLGEN updates the DBCONFIG member  
that contains the SMF record types used by the  
CA MICS Network Analyzer.

REFERENCES: Chapter 7 of this guide

**SNT00147**

```
+-----+
| S N T 0 0 1 4 7 |
+-----+
```

TEXT: TELNET SERVER SUSPENDED LOGF RECORDS MOVED TO  
TCPSTN01 FILE.

TYPE: Information

REASON: TCP/IP Telnet Server Suspend File, holds LOGN  
records for which no LOGF record is received yet  
or LOGN record for which no LOGN record is found  
yet. The data stored in the suspend file  
remains there until it exceeds the limit  
specified via TCPLIMIT option in PARMS(SNTOPS).  
When this occurs, the LOGF observation from the  
TCPTSS01 file will be moved to TCPSTN01 file.  
The message displays the total number of LOGF  
records moved to STN file during that DAILY run.

ACTION: None

REFERENCES: Chapter 7 of this guide

## SNT00148

```
+-----+
| S N T 0 0 1 4 8 |
+-----+
```

TEXT: API SUSPENDED TERM RECORDS MOVED TO TCPAPI01.

TYPE: Information

REASON: TCP/IP API Calls for Sockets Suspend File, which holds INIT records for which no TERM record is received yet or TERM record for which no INIT record is found yet. The data stored in the suspend file remains there until it exceeds the limit specified via TCPLIMIT option in PARMS(SNTOPS). When this occurs, the LOGF observation from the TCPSAP01 file will be moved to TCPAPI01 file. The message displays the total number of TERM records moved to API file during that DAILY run.

ACTION: None

REFERENCES: Chapter 7 of this guide

**SNT00149**

```
+-----+
| S N T 0 0 1 4 9 |
+-----+
```

TEXT: TELNET SERVER SUSPENDED LOGN RECORDS DROPPED.

TYPE: Information

REASON: TCP/IP Telnet Server Suspend File (TSS), which holds LOGN records for which no LOGF record is received yet or LOGF record for which no LOGN record is found yet. The data stored in the suspend file remains there until it exceeds the limit specified via TCPLIMIT option in PARMS(SNTOPS). When this occurs, the LOGN observations will be dropped from TCPTSS01 file. The message displays the total number of LOGN records dropped from the TSS file during that DAILY run.

ACTION: None

REFERENCES: Chapter 7 of this guide

## SNT00150

```
+-----+
| S N T 0 0 1 5 0 |
+-----+
```

TEXT: API SUSPENDED INIT RECORDS DROPPED.

TYPE: Information

REASON: TCP/IP API Calls for Sockets Suspend File (SAP), which holds INIT records for which no TERM record is received yet or TERM record for which no INIT record is found yet. The data stored in the suspend file remains there until it exceeds the limit specified via TCPLIMIT option in PARMS(SNTOPS). When this occurs, the INIT observations will be dropped from TCPSAP01 file. The message displays the total number of INIT records dropped from SAP file during that DAILY run.

ACTION: None

REFERENCES: Chapter 7 of this guide



**\$HEDE SNT00151**

```
+-----+
| S N T 0 0 1 5 1 |
+-----+
```

TEXT:       \*\* INDICATES THIS ORGSYSID IS RECOGNIZED IN THE  
              INPUT DATA BECAUSE ???? IS CODED FOR ORGSYSID  
              IN SNTOPS.

TYPE:       Information

REASON:     After all input records are read in the DAILY  
              job, this message is used to produce a report  
              in the MICSLLOG outlining the SYSID's that were  
              recognized in the input data because ???? is  
              coded for ORGSYSID in SNTOPS. A ???? parameter  
              for ORGSYSID directs the DAILY step to  
              recognize SMF data from original systems that  
              are not explicitly defined.

ACTION:     Review additional MICSLLOG reports to determine  
              if the proper data is being read and processed  
              in the DAILY job.

REFERENCES: Chapter 7 of this guide

**SNT00200**

```
+-----+
| S N T 0 0 2 0 0 |
+-----+
```

TEXT:       >>>> NETWORK COMPONENT REPORT GENERATOR  
              >>>> REPORT LIST INPUT:

TYPE:       Information

REASON:     The CA MICS Network Analyzer is shipped with a  
              complete report generation program. This  
              message is issued as the parsing of the report  
              request cards begins. It is followed by  
              SNT00217, which shows the actual report request  
              card.

ACTION:     None

REFERENCES: None

## SNT00201

```
+-----+
| S N T 0 0 2 0 1 |
+-----+
```

TEXT: >ERR> REPORT NAME SPECIFIED: '%KEYWORD2 IS  
LONGER THAN 6 CHARACTERS.'

TYPE: Error

REASON: The CA MICS Network Analyzer report generator  
(GNSNTRPT) requires the second keyword on the  
REPORT statement to contain a six-position  
report ID. This message is issued when the  
report ID does not equal six positions.

ACTION: Modify the Report-ID field on the REPORT card to  
contain a valid six-position report identifier.

REFERENCES: Chapter 3 of this guide

## SNT00202

```
+-----+
| S N T 0 0 2 0 2 |
+-----+
```

TEXT: REPORT NAME IS INVALID.  
REPORT NAME SPECIFIED: %KEYWORD2  
POSITIONS 4-6 MUST BE NUMERIC.

TYPE: Error

REASON: The CA MICS Network Analyzer report generator  
(GNSNTRPT) requires that positions four through  
six of each REPORT statement's report ID keyword  
be numeric. This message is issued when these  
positions are not numeric.

ACTION: Modify the Report-ID field to contain valid  
numeric values in positions four through six.

REFERENCES: Chapter 3 of this guide

## SNT00203

```
+-----+
| S N T 0 0 2 0 3 |
+-----+
```

TEXT:       INVALID REPORT SPECIFIED: %KEYWORD2  
              VALID SERVICE REPORTS ARE:  
              SNT101, SNT103, SNT105, SNT111, SNT112,  
              SNT113, AND SNT114, SNT121, AND SNT122.

TYPE:        Error

REASON:      The CA MICS Network Analyzer report generator  
              (GNSNTRPT) contains specific service reports  
              that have a report ID in the form SNT1xx, where  
              xx is the report number. This message is issued  
              if the report number does not match an internal  
              table that contains the valid IDs shown in the  
              message text.

ACTION:      Correct the service report number.

REFERENCES:   Chapter 3 of this guide

## SNT00204

```
+-----+
| S N T 0 0 2 0 4 |
+-----+
```

TEXT:        REPORT %WKRPRT ONLY VALID IN DETAIL TIME-SPAN.  
              USER REQUESTED TIME SPAN: %KEYWORD4

TYPE:        Error

REASON:      The CA MICS Network Analyzer report  
              generator (GNSNTRPT) produces report SNT113  
              based on data from the NVSRTM File data element  
              SLUPU. In this file, SLUPU does not exist  
              beyond the DETAIL timespan. This message is  
              issued when you request the SNT113 report in any  
              timespan other than X.

ACTION:      Specify X as the timespan for the SNT113  
              report.

REFERENCES:   Chapter 3 of this guide

## SNT00205

```
+-----+
| S N T 0 0 2 0 5 |
+-----+
```

TEXT:           INVALID REPORT SPECIFIED: %KEYWORD2  
                  VALID WORKLOAD REPORTS ARE:  
                  SNT201, SNT203, SNT208, SNT209, SNT211,  
                  SNT212, SNT213, AND SNT214, SNT221, AND SNT222.

TYPE:           Error

REASON:          The CA MICS Network Analyzer report  
                  generator (GNSNTRPT) contains specific workload  
                  reports that have report IDs in the form SNT2xx,  
                  where xx is the report number. This message is  
                  issued if the report number does not match an  
                  internal table that contains the valid IDs shown  
                  in the message text.

ACTION:          Modify the workload report number to be a valid  
                  report ID.

REFERENCES:      Chapter 3 of this guide

**SNT00206**

```
+-----+
| S N T 0 0 2 0 6 |
+-----+
```

TEXT:       INVALID REPORT SPECIFIED: %KEYWORD2  
              VALID DATA COLLECTION REPORTS ARE:  
              SNT401 AND SNT403.

TYPE:        Error

REASON:      The CA MICS Network Analyzer's report  
              generator (GNSNTRPT) contains specific data  
              collection reports that have report IDs in the  
              form SNT4xx, where xx is the report number.  
              This message is issued if the report number does  
              not match an internal table that contains the  
              valid IDs shown in the message text.

ACTION:      Modify the data collection report number to  
              contain a valid report ID.

REFERENCES:   Chapter 3 of this guide

**SNT00207**

```
+-----+
| S N T 0 0 2 0 7 |
+-----+
```

TEXT:       INVALID REPORT SPECIFIED: %KEYWORD2  
              VALID INCIDENT ANALYSIS REPORTS ARE:  
              SNT601 AND SNT602.

TYPE:        Error

REASON:      The CA MICS Network Analyzer report  
              generator (GNSNTRPT) contains specific incident  
              analysis reports that have report ID in the form  
              SNT6xx, where xx is the report number. This  
              message is issued if the report number does not  
              match an internal table that contains the valid  
              IDs shown in the message text.

ACTION:      Modify the incident analysis report number to  
              contain a valid report ID.

REFERENCES:   Chapter 3 of this guide

## SNT00208

```
+-----+
| S N T 0 0 2 0 8 |
+-----+
```

TEXT:           INVALID REPORT CLASS SPECIFIED: %RPTCLASS  
                  VALID REPORT CLASSES ARE:  
                  SNT1XX, SNT2XX, SNT4XX, AND SNT6XX

TYPE:           Error

REASON:          The CA MICS Network Analyzer report  
                  generator (GNSNTRPT) contains specific report  
                  classes. Position 4 of the report ID indicates  
                  the report class. This message is displayed if  
                  the report class does not match an internal  
                  table that contains the valid IDs shown in the  
                  message text.

ACTION:          Modify the report class to contain a valid  
                  report ID.

REFERENCES:      Chapter 3 of this guide

## SNT00209

```
+-----+
| S N T 0 0 2 0 9 |
+-----+
```

TEXT:           REPORT NAME DOES NOT BEGIN WITH THE CHARACTERS  
                  -SNT- REPORT NAME SPECIFIED: %KEYWORD2

TYPE:           Error

REASON:          The first three positions of the report ID  
                  keyword specified on the report statement for  
                  the CA MICS Network Analyzer report  
                  generator (GNSNTRPT) must contain SNT. This  
                  message is issued when the first three positions  
                  do not contain SNT.

ACTION:          Code SNT as the prefix for the report ID.

REFERENCES:      Chapter 3 of this guide

## SNT00210

```
+-----+
| S N T 0 0 2 1 0 |
+-----+
```

TEXT: UNKNOWN REPORT FORMAT SPECIFIED ==> %KEYWORD3.  
VALID FORMATS ARE - PROFILE - AND - TREND -

TYPE: Error

REASON: The CA MICS Network Analyzer report generator (GNSNTRPT) produces either profile or trend format reports when you specify PROFILE or TREND, respectively, for the report format parameter. This message is issued if you do not specify PROFILE or TREND for the format parameter.

ACTION: Specify the correct value for format parameter.

REFERENCES: Chapter 3 of this guide

## SNT00211

```
+-----+
| S N T 0 0 2 1 1 |
+-----+
```

TEXT: INVALID TIME-SPAN SPECIFIED ==> %KEYWORD4  
VALID VALUES ARE - X, D, W, M, AND Y -

TYPE: Error

REASON: The CA MICS Network Analyzer report generator (GNSNTRPT) produces reports from any of the timespans that CA MICS supports by coding the timespan parameter on the report statement. This message is displayed if the timespan parameter is not equal to X (DETAIL), D (DAYS), W (WEEKS), M (MONTHS), or Y (YEARS).

ACTION: Specify the correct value for the timespan parameter.

REFERENCES: Chapter 3 of this guide

## SNT00212

```
+-----+
| S N T 0 0 2 1 2 |
+-----+
```

TEXT:           STARTING CYCLE IS NON-NUMERIC.  
                  STARTING CYCLE SPECIFIED: %KEYWORD5  
                  A STARTING CYCLE OF 01 HAS BEEN ASSUMED.

TYPE:           Error

REASON:          The CA MICS Network Analyzer report generator  
                  (GNSNTRPT) produces reports from any cycle in an  
                  existing CA MICS file. The cycle to be used for  
                  the report is specified as the cycle parameter  
                  on the report statement. This message is issued  
                  if the cycle parameter is not numeric.

ACTION:          Specify a valid number for the cycle parameter  
                  (for example, a number that is in the range of  
                  the number of cycles CA MICS keeps for the  
                  file).

REFERENCES:      Chapter 3 of this guide

## SNT00213

```
+-----+
| S N T 0 0 2 1 3 |
+-----+
```

TEXT:           KEYWORD NOT RECOGNIZED. KEYWORD = %KEYWORD1.

TYPE:           Error

REASON:          The first keyword on the report statement for a  
                  profile or trend report must be REPORT. This  
                  message is issued if REPORT is not the first  
                  keyword.

ACTION:          Specify REPORT as the first keyword.

REFERENCES:      Chapter 3 of this guide



**SNT00214**

```
+-----+
| S N T 0 0 2 1 4 |
+-----+
```

TEXT: THIS REPORT BYPASSED DUE TO PARAMETER ERRORS.

TYPE: Warning

REASON: This message is issued when the CA MICS Network Analyzer report generator (GNSNTRPT) finds one or more errors on a report control card. The report that was bypassed is shown on the previous display of the SNT00217 message.

ACTION: None

REFERENCES: Chapter 3 of this guide

**SNT00215**

```
+-----+
| S N T 0 0 2 1 5 |
+-----+
```

TEXT: >>>> END OF REPORT LIST INPUT.

TYPE: Information

REASON: This message is issued after the CA MICS Network Analyzer report generator (GNSNTRPT) completes parsing the report control statements.

ACTION: None

REFERENCES: Chapter 3 of this guide

## SNT00216

```
+-----+
| S N T 0 0 2 1 6 |
+-----+
```

TEXT:           NUMBER OF ERRORS IN REPORT LIST PARAMETERS  
                  = %CHARNUM  
                  SOME REPORTS WERE NOT GENERATED.  
                  CORRECT ERROR(S) AND EXECUTE AGAIN.

TYPE:           Error

REASON:          The CA MICS Network Analyzer report generator  
                  (GNSNTRPT) issues this message if one or more  
                  errors are found while parsing the report  
                  control statements.

ACTION:          Correct errors identified by previous messages  
                  and resubmit the job for execution.

REFERENCES:      Chapter 3 of this guide

## SNT00217

```
+-----+
| S N T 0 0 2 1 7 |
+-----+
```

TEXT:           ' %LINE ' (the value of %LINE without the  
                  quotes).

TYPE:           Information

REASON:          This message is issued each time the CA MICS  
                  Network Analyzer report generator (GNSNTRPT)  
                  begins parsing a report control statement. The  
                  value of the complete control statement that you  
                  code equals the value of %LINE.

ACTION:          None

REFERENCES:      Chapter 3 of this guide

**SNT00218**

```
+-----+
| S N T 0 0 2 1 8 |
+-----+
```

TEXT: REPORT %REPORT; THE LABEL FOR %ACTVAR HAS BEEN  
CHANGED.

TYPE: Error

REASON: The CA MICS Network Analyzer produces two  
reports based on the data element SNTACT3.  
Normally, the value of SNTACT3 equals the value  
in the data element Secondary Logical Unit  
Physical Unit (SLUPU). You may change this  
value using the SNTACCT parameter and SNTACRT  
exit. If you do this, the two reports are no  
longer valid and the report generator (GNSNTRPT)  
checks the SAS label on SNTACT3. This message  
is issued if the value of SNTACT3 is not the  
same as the default value (SLUPU) shipped by CA.

ACTION: If your site requires the SNT113 and SNT213  
reports, you must restore the value of SNTACT3  
to the default value (SLUPU).

REFERENCES: See Chapter 3 of this guide for information  
regarding the reports, and Chapter 7 for a  
discussion of the SNTACCT and SNTACRT  
parameters.

## SNT00300

```
+-----+
| S N T 0 0 3 0 0 |
+-----+
```

TEXT: ' %LINE ' (the value of %LINE without the quotes).

TYPE: Information

REASON: This message is issued each time the CA MICS Network Analyzer parameter generator (SNTPGEN) begins parsing the control statement. The value of the complete control statement that you code equals the value of %LINE.

ACTION: None

REFERENCES: Chapter 7 of this guide

**SNT00301**

```
+-----+
| S N T 0 0 3 0 1 |
+-----+
```

TEXT:           LENGTH OF KEYWORD GREATER THAN 17.  
                  KEYWORD = %KEYWORD

TYPE:           Error

REASON:         The CA MICS Network Analyzer parameter generator (SNTPGEN) brings together the first and second words of each input line to construct a keyword (some keywords contain two words, for example, DATA SOURCES). The parsing routine then determines if the length of both combined is greater than 17 positions. If the length is greater than 17, no further parsing is done, this message is issued, and the line is flagged as an error.

ACTION:         Check the lengths of the first two words in the input line. Neither word length should exceed eight positions, so that when they are combined with one blank in between, the combined length does not exceed 17 positions.

REFERENCES:     Chapter 7 of this guide

## SNT00302

```
+-----+
| S N T 0 0 3 0 2 |
+-----+
```

TEXT:           INVALID KEYWORD(S) ON INPUT RECORD.  
                  FOUND: %KEYWORD  
                  SEE COMPLETE LIST OF VALID KEYWORDS AT THE END  
                  OF MICSLOG.

TYPE:           Error

REASON:          The CA MICS Network Analyzer parameter generator  
                  (SNTPGEN) scans an internal table to determine  
                  whether a keyword is valid. This message is  
                  issued if the keyword is invalid. The message  
                  prints out the invalid keyword and SNT00303,  
                  which immediately follows SNT00302, prints out a  
                  list of valid keywords.

ACTION:          Determine the proper keyword for this statement  
                  and modify it.

REFERENCES:      Chapter 7 of this guide

## SNT00303

```
+-----+
| S N T 0 0 3 0 3 |
+-----+
```

TEXT:           ' %V\_TOK '  
                  (where %V\_TOK will represent a valid keyword)

TYPE:           Information

REASON:          This message always follows SNT00302. See  
                  SNT00302 for a description of the conditions  
                  under which this message is issued. The  
                  CA MICS Network Analyzer parameter generation  
                  program issues one SNT00303 message for each  
                  valid keyword.

ACTION:          Determine the proper keyword for this statement  
                  and modify it.

REFERENCES:      Chapter 7 of this guide

**SNT00304**

```
+-----+
| S N T 0 0 3 0 4 |
+-----+
```

TEXT: NETWORK ID STATEMENT NOT FOUND OR PARM NOT CODED.

TYPE: Error

REASON: The CA MICS Network Analyzer parameter generation program requires that you provide a NETWORK ID statement containing a valid parameter in the SNTOPS. This message is issued when either is absent.

ACTION: Code a valid NETWORK ID statement in SNTOPS.

REFERENCES: Chapter 7 of this guide

**SNT00305**

```
+-----+
| S N T 0 0 3 0 5 |
+-----+
```

TEXT: ORGSYSID PARM RECEIVED BEFORE NETWORK ID PARM.

TYPE: Error

REASON: The CA MICS Network Analyzer parameter generation program requires that you code the NETWORK ID keyword immediately before the ORGSYSID keyword. This message is issued if ORGSYSID is found before a valid NETWORK ID.

ACTION: Code the NETWORK ID keyword before the ORGSYSID keyword.

REFERENCES: Chapter 7 of this guide

## SNT00306

```
+-----+
| S N T 0 0 3 0 6 |
+-----+
```

TEXT: ORGSYSID STATEMENT NOT FOUND OR PARM NOT CODED.

TYPE: Error

REASON: The CA MICS Network Analyzer parameter generation program requires that you provide an ORGSYSID statement containing a valid parameter in the SNTOPS parameter. This message is issued when either is absent.

ACTION: Code a valid ORGSYSID statement in SNTOPS.

REFERENCES: Chapter 7 of this guide

## SNT00307

```
+-----+
| S N T 0 0 3 0 7 |
+-----+
```

TEXT: TIME OFFSET STATEMENT FOUND OUT OF ORDER.

TYPE: Error

REASON: The CA MICS Network Analyzer parameter generation program requires that you code the ORGSYSID statement immediately before the TIME OFFSET statement. This message is issued if TIME OFFSET is found before a valid ORGSYSID.

ACTION: Code the ORGSYSID statement before the TIME OFFSET statement.

REFERENCES: Chapter 7 of this guide



**SNT00308**

```
+-----+
| S N T 0 0 3 0 8 |
+-----+
```

TEXT: TIME OFFSET VALUE NOT CODED OR INVALID DATA.

TYPE: Error

REASON: The CA MICS Network Analyzer parameter generation program requires that you code the TIME OFFSET keyword. This message is issued if you do not code the TIME OFFSET keyword, or if the offset value is not numeric.

ACTION: Code the TIME OFFSET keyword and a valid numeric value (-12 to 12).

REFERENCES: Chapter 7 of this guide

**SNT00309**

```
+-----+
| S N T 0 0 3 0 9 |
+-----+
```

TEXT: TIME OFFSET LESS THAN -12 OR GREATER THAN +12 .

TYPE: Error

REASON: The TIME OFFSET keyword contains a time value (in hours) that is used to adjust input timestamps. Since the value represents relative hours (not military time), the value cannot be greater than +12 or less than -12. This message is issued if the value falls outside that range.

ACTION: Code a value that is less than or equal to +12 and greater than or equal to -12.

REFERENCES: Chapter 7 of this guide

## SNT00310

```
+-----+
| S N T 0 0 3 1 0 |
+-----+
```

TEXT: INVALID DATA SOURCE VALUE. %DATASRCT

TYPE: Error

REASON: The DATA SOURCES keyword in the SNTOPS parameter contains the data sources needed for processing. The valid entries are the following:

NPMM, NPMS, NLDM, NPDA, NSPY, NTS, NEWS

This message is issued when a source (name) other than one of those listed above is found.

ACTION: Code one or more of the data source names listed above. You may code them in any sequence.

REFERENCES: Chapter 7 of this guide

## SNT00311

```
+-----+
| S N T 0 0 3 1 1 |
+-----+
```

TEXT: SESSION MANAGER PARM FOUND BEFORE DATA SOURCES.

TYPE: Error

REASON: The DATA SOURCES keyword in the SNTOPS parameter must precede the SESSION MANAGER keyword parameter.

ACTION: Probable cause is that either the DATA SOURCES keyword parameter is missing or the parameters are out of sequence. The SESSION MANAGER keyword parameter must follow the DATA SOURCES parameter.

REFERENCES: Chapter 7 of this guide for proper coding of the SNTOPS member.

**SNT00312**

```
+-----+
| S N T 0 0 3 1 2 |
+-----+
```

TEXT:           INVALID MULTI-SESSION MANAGER DELETE VALUE.  
                  DELETEMS VALUE BLANK  
                  or  
                  INVALID MULTI-SESSION MANAGER DELETE VALUE.  
                  INVALID VALUE ON DELETEMS STATEMENT.

TYPE:           Error

REASON:          The DELETEMS statement of the SNTOPS parameter  
                  is an optional statement that, if coded, must be  
                  the value Y, YES, N, or NO.

ACTION:          Put the desired and correct value on the  
                  statement.

REFERENCES:      Chapter 7 of this guide for proper coding of the  
                  SNTOPS member.

**SNT00313**

```
+-----+
| S N T 0 0 3 1 3 |
+-----+
```

TEXT:           ORGSYSID STATEMENT FOUND OUT OF ORDER.

TYPE:           Error

REASON:          The ORGSYSID statement of the SNTOPS parameter  
                  must follow either the NETWRKID, DATA SOURCES,  
                  IBMTCP SMF, NETSPY SMF, or NETTCP SMF statement.

ACTION:          Code the ORGSYSID in a proper order as mentioned  
                  in the REASON section above.

REFERENCES:      Chapter 7 of this guide for proper coding of the  
                  SNTOPS member.

## SNT00314

```
+-----+
| S N T 0 0 3 1 4 |
+-----+
```

TEXT: DATA SOURCE CODED MORE THAN ONCE. %DATASRCT

TYPE: Error

REASON: The DATA SOURCES statement in the SNTOPS parameter generation contains the data sources needed for processing. This message is issued if a data source is coded more than once on one specific DATA SOURCES keyword.

ACTION: Delete the duplicated data source.

REFERENCES: Chapter 7 of this guide

## SNT00317

```
+-----+
| S N T 0 0 3 1 7 |
+-----+
```

TEXT: DATA SOURCES STATEMENT NOT FOUND.

TYPE: Error

REASON: The CA MICS Network Analyzer parameter generation program requires that you provide a DATA SOURCES statement in the SNTOPS parameter. This message is issued when it is absent.

ACTION: Code a valid DATA SOURCES statement in SNTOPS.

REFERENCES: Chapter 7 of this guide

**SNT00318**

```
+-----+
| S N T 0 0 3 1 8 |
+-----+
```

TEXT: ERRORS FOUND ON INPUT PARAMETERS. CORRECT AND RESUBMIT.

TYPE: Error

REASON: One or more errors were found during the parsing of the input parameter by the CA MICS Network Analyzer parameter generation program. The run aborts after this message is issued three times.

ACTION: Correct the errors found in MICSLOG.

REFERENCES: Chapter 7 of this guide

**SNT00319**

```
+-----+
| S N T 0 0 3 1 9 |
+-----+
```

TEXT: SCAN OF NETWORK SERVICE GROUP PARAMETERS AT %CGENTS

TYPE: Information

REASON: One of the phases of the CA MICS Network Analyzer parameter generation program is to parse the network service group parameter to build the proper tables. This message is issued at the beginning of the parsing process.

ACTION: None

REFERENCES: None

## SNT00320

```
+-----+
| S N T 0 0 3 2 0 |
+-----+
```

TEXT:            '%LINE72 '

TYPE:            Information

REASON:          This message is issued each time the CA MICS  
Network Analyzer parameter generator (SNTPGEN)  
begins the parsing of network service group  
statements. The value of the complete control  
statement that you code equals the value of  
%LINE72.

ACTION:          None

REFERENCES:      Chapter 7 of this guide

## SNT00321

```
+-----+
| S N T 0 0 3 2 1 |
+-----+
```

TEXT:            KEYWORD 1 NOT EQUAL TO "GROUP"

TYPE:            Error

REASON:          As the CA MICS Network Analyzer parameter  
generator (SNTPGEN) parses the network service  
group statements, the first keyword (token) on  
each statement must be GROUP. This message is  
issued if the keyword is not GROUP.

ACTION:          Modify the statement to begin with GROUP.

REFERENCES:      Chapter 7 of this guide

**SNT00322**

```
+-----+
| S N T 0 0 3 2 2 |
+-----+
```

TEXT: KEYWORD %KEYWRD NOT NUMERIC.

TYPE: Error

REASON: As the CA MICS Network Analyzer parameter generator (SNTPGEN) parses the network service group statements, the network service group number (second token) on each statement must be numeric. This message is issued if the network service group number is not numeric.

ACTION: Modify the network service group number to be numeric.

REFERENCES: Chapter 7 of this guide

**SNT00323**

```
+-----+
| S N T 0 0 3 2 3 |
+-----+
```

TEXT: NETWORK SERVICE GROUP NUMBER CAN NOT EXCEED 256.

TYPE: Error

REASON: The value of the network service group number exceeded 256.

ACTION: Modify the value for network service group number so that it contains a number between 1 and 256, inclusive.

REFERENCES: Chapter 7 of this guide

## SNT00324

```
+-----+
| S N T 0 0 3 2 4 |
+-----+
```

TEXT: THE INDEX TO THE CONTROL ARRAYS EXCEEDED 256.  
PROBABLE CAUSE: VALID INPUT LINE COUNT GREATER THAN 256.

TYPE: Error

REASON: Prefix.MICS.PARMS(NETGROUP) cannot contain more than 256 entries. This message is issued when the Network Analyzer parameter generation program (SNTPGEN) finds more than 256 entries.

ACTION: Delete the entries in excess of 256 in prefix.MICS.PARMS(NETGROUP). Valid values are 1 through 256.

REFERENCES: Chapter 7 of this guide

## SNT00325

```
+-----+
| S N T 0 0 3 2 5 |
+-----+
```

TEXT: ABORT>> %INERR ERRORS FOUND DURING SCREENING OF NETWORK SERVICE GROUP PARAMETERS.

TYPE: Error

REASON: This message is issued if the CA MICS Network Analyzer parameter generation program (SNTPGEN) finds one or more errors during the parsing of the network service group statements.

ACTION: Locate and correct all of the errors. (You can find a listing of error message in MICSLOG.)

REFERENCES: Chapter 7 of this guide



**SNT00326**

```
+-----+
| S N T 0 0 3 2 6 |
+-----+
```

TEXT: SCAN OF NETWORK APPLICATION TABLE ENTRIES AT  
%CGENTS

TYPE: Information

REASON: This message is issued as the CA MICS Network  
Analyzer parameter generation program (SNTPGEN)  
begins to parse the Network Application (PLU)  
parameter to build the proper tables.

ACTION: None

REFERENCES: Chapter 7 of this guide

**SNT00327**

```
+-----+
| S N T 0 0 3 2 7 |
+-----+
```

TEXT: ABORT>> THE INDEX TO THE CONTROL ARRAY EXCEEDED  
999.  
PROBABLE CAUSE: VALID INPUT LINE COUNT  
GREATER THAN 999 FOR THE NETWORK APPLICATION  
TABLE.

TYPE: Error

REASON: Prefix.MICS.PARMS(NETAPPL) cannot contain more  
than 999 entries. This message is issued when  
the CA MICS Network Analyzer parameter  
generation program (SNTPGEN) finds more than 999  
entries.

ACTION: Delete the entries in excess of 999 in  
prefix.MICS.PARMS(NETAPPL).

REFERENCES: Chapter 7 of this guide

## SNT00328

```
+-----+
| S N T 0 0 3 2 8 |
+-----+
```

TEXT:            --->%KEYWORD PARM VALUE NOT CODED OR INVALID  
                 DATA.

TYPE:            Error

REASON:          The keyword parameter value is either not  
                 defined or contains an invalid value.

ACTION:          Code the correct value for the KEYWORD in  
                 prefix.MICS.PARMS(SNTOPS) and resubmit the job.

REFERENCES:      Chapter 7 of this guide

## SNT00329

```
+-----+
| S N T 0 0 3 2 9 |
+-----+
```

TEXT:            %KEYWORD IS LESS THAN 1 OR GREATER THAN 365.

TYPE:            Error

REASON:          The keyword parameter value contains negative  
                 value or some value that is greater than 365.  
                 This value must be positive ranging from 1 to  
                 365.

ACTION:          Code the correct value for the KEYWORD in  
                 prefix.MICS.PARMS(SNTOPS) and resubmit the job.

REFERENCES:      Chapter 7 of this guide

## SNT00330

```
+-----+
| S N T 0 0 3 3 0 |
+-----+
```

TEXT:           STATEMENT : %LINE FOLLOWING DATA SOURCES CODED  
                  IN THE STATEMENT ABOVE ARE CONSIDERED INACTIVE  
                  BECAUSE THEIR ASSOCIATED FILES ARE TURNED OFF  
                  IN SHAREDPREFIX.MICS.GENLIB(SNTGENIN).  
                  %DATASRC  
                  PLEASE REMOVE INACTIVE DATA SOURCE(S) FROM THE  
                  STATEMENT ABOVE AND RESUBMIT  
                  PREFIX.MICS.PARMS(SNTPGEN). REFER TO APPENDIX  
                  A OF CA MICS RESOURCE MANAGEMENT NETWORK OPTION  
                  GUIDE FOR MORE DETAILS ABOUT THIS MESSAGE.

TYPE:           Error

REASON:          One or more of the data sources (NPDA, NLDM,  
                  NPMS, or TCP), as indicated in the message text,  
                  was found in prefix.MICS.PARMS(SNTOPS) whose  
                  associated files are all turned off. To improve  
                  performance, CPU utilization, and execution  
                  time, the processing code for each data source  
                  defined in prefix.MICS.PARMS(SNTOPS) is included  
                  during the DAY056 step execution. If a data  
                  source is required for your site, you should not  
                  define it in prefix.MICS.PARMS(SNTOPS).

Following is a list of files associated with  
each data source along with the record type.

| Data Source | SMF Recd Type | Files and Description                                                                                                                                                                                                                                          |
|-------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NPDA        | 37            | LNF LAN File<br>GAF Generic Alert File<br>NEF NPDA Event File<br>NSF NPDA Statistical File                                                                                                                                                                     |
| NLDM        | 39            | NSV NLDM Service File<br>LSY NLDM System (PLU) Activity File<br>NLL NLDM Link Activity File<br>VBF NLDM VTAM Bind Failure File<br>NSC NLDM Session Connectivity File<br>RTE NLDM Route File<br>RTM NLDM Response Time File<br>NSA NLDM Session Accounting File |

NPMS 28 PSU NPM User Activity File  
Subtypes(32, PSY NPM System (PLU) Activity File  
80-82,96-98) NPL NPM Link Activity File

TCP 118,119 STN Telnet Server File  
CTN Telnet Client File  
FSF FTP Server File  
FLF FTP Login Failure File  
FCF FTP Client File  
API API Calls for Sockets File

ACTION: Remove the data sources as indicated in the  
message text from all statements and resubmit  
the prefix.MICS.CNTL(SNTPGEN).

REFERENCES: Chapter 7 of this guide

## SNT00331

```
+-----+
| S N T 0 0 3 3 1 |
+-----+
```

TEXT: SMF RECORD NUMBER IS MISSING FROM THE  
STATEMENT. PLEASE CODE %TOK\_CHK9 RECORD NUMBER  
TO CONTINUE. REFER TO APPENDIX A OF CA MICS  
RESOURCE MANAGEMENT NETWORK OPTION GUIDE FOR  
MORE DETAILS ABOUT THIS MESSAGE.

TYPE: Error

REASON: As indicated in the message text, the NETSPY SMF  
parameter requires an SMF record number (for  
example, 132) that is not found in the statement  
above. You must code a valid CA NetSpy SMF  
record number in the range of 128 - 255.

ACTION: Edit prefix.MICS.PARMS(SNTOPS), specify the SMF  
record number referenced in the error message,  
and resubmit the prefix.MICS.CNTL(SNTPGEN).

REFERENCES: Chapter 7 of this guide

**SNT00332**

```
+-----+
| S N T 0 0 3 3 2 |
+-----+
```

**TEXT:** SMF RECORD NUMBER IS MISSING FROM THE STATEMENT. PLEASE CODE %TOK\_CK10 RECORD NUMBER TO CONTINUE. REFER TO APPENDIX A OF CA MICS RESOURCE MANAGEMENT NETWORK OPTION GUIDE FOR MORE DETAILS ABOUT THIS MESSAGE.

**TYPE:** Error

**REASON:** As indicated in the message text, the NETTCP SMF parameter requires an SMF record number (for example, 132) that is not found. You must code a valid CA Netmaster for TCP/IP SMF record number in the range of 128 - 255.

**ACTION:** Edit prefix.MICS.PARMS(SNTOPS), specify the SMF record number referenced in the error message, and resubmit the prefix.MICS.CNTL(SNTPGEN).

**REFERENCES:** Chapter 7 of this guide

## SNT00333

```
+-----+
| S N T 0 0 3 3 3 |
+-----+
```

TEXT: THE NSPY SMF RECORD NUMBER %NSPYRTYP DECLARED IS NOT DEFINED IN SP.MICS.GENLIB(SNTGENIN) INPUTSOURCE STATEMENT. PLEASE REFER TO DETAIL MESSAGE DESCRIPTION IN APPENDIX A OF CA MICS RESOURCE MANAGEMENT NETWORK OPTION GUIDE FOR MORE INFORMATION.

TYPE: Error

REASON: The SMF record number specified for NSPY option with NETSPY SMF = nnn statement is not defined in the sharedprefix.MICS.GENLIB(SNTGENIN) INPUTSOURCE statement.

ACTION: Edit sharedprefix.MICS.GENLIB(SNTGENIN) and specify the SMF record number displayed in the message text.

Submit sharedprefix.MICS.CNTL(SNTCGEN)

After the SNTCGEN completes successfully, edit prefix.MICS.PARMS(JCLGENU) so that it contains no keywords (is a blank member); then submit prefix.MICS.CNTL(JCLGENU).

Resubmit the prefix.MICS.CNTL(SNTPGEN).

REFERENCES: Chapter 7 of this guide

**SNT00334**

```
+-----+
| S N T 0 0 3 3 4 |
+-----+
```

TEXT: THE NTCIP SMF RECORD NUMBER %NTCPRTPY DECLARED IS NOT DEFINED IN SP.MICS.GENLIB(SNTGENIN) INPUTSOURCE STATEMENT. PLEASE REFER TO DETAIL MESSAGE DESCRIPTION IN APPENDIX A OF CA MICS RESOURCE MANAGEMENT NETWORK OPTION GUIDE FOR MORE INFORMATION.

TYPE: Error

REASON: The SMF record number specified for NSPY option with NETSPY SMF = nnn statement is not defined in the sharedprefix.MICS.GENLIB(SNTGENIN) INPUTSOURCE statement.

ACTION: Edit sharedprefix.MICS.GENLIB(SNTGENIN) and specify the SMF record number displayed in the message text.

Submit sharedprefix.MICS.CNTL(SNTCGEN)

After the SNTCGEN completes successfully, edit prefix.MICS.PARMS(JCLGENU) so that it contains no keywords (is a blank member); then submit prefix.MICS.CNTL(JCLGENU).

Resubmit the prefix.MICS.CNTL(SNTPGEN).

REFERENCES: Chapter 7 of this guide

## SNT00335

```
+-----+
| S N T 0 0 3 3 5 |
+-----+
```

TEXT: NETSPY SMF = NNN STATEMENT FOUND AFTER A DATA SOURCE STATEMENT THAT DID NOT SPECIFY NSPY OPTION OR THIS STATEMENT IS DEFINED MULTIPLE TIMES.

TYPE: Error

REASON: The NSPY option was not used in the DATA SOURCE statement that preceded the NETSPY SMF = nnn statement (which is used to declare the SMF record number for the NSPY data source). Another reason this message could be seen is that there may be a duplicate NETSPY SMF = nnn statement.

ACTION: Edit prefix.MICS.PARMS(SNTOPS) and remove the statement in question, or specify the NSPY option on the preceding DATA SOURCE statement.

Resubmit the prefix.MICS.CNTL(SNTPGEN).

REFERENCES: Chapter 7 of this guide



**SNT00336**

```
+-----+
| S N T 0 0 3 3 6 |
+-----+
```

TEXT: NETTCP SMF = NNN STATEMENT FOUND AFTER A DATA SOURCE STATEMENT THAT DID NOT SPECIFY NTCP OPTION OR THIS STATEMENT IS DEFINED MULTIPLE TIMES.

TYPE: Error

REASON: The NTCP option was not used in the DATA SOURCE statement that preceded the NETSPY SMF = nnn statement (which is used to declare the SMF record number for the NSPY data source). Another reason this message could be seen is that there may be a duplicate NETTCP SMF = nnn statement.

ACTION: Edit prefix.MICS.PARMS(SNTOPS) and remove the statement in question, or specify the NTCP option on the preceding DATA SOURCE statement.

Resubmit the prefix.MICS.CNTL(SNTPGEN).

REFERENCES: Chapter 7 of this guide

## SNT00337

```
+-----+
| S N T 0 0 3 3 7 |
+-----+
```

TEXT:           PREVIOUS DATA SOURCE STATEMENT CONTAINED NSPY  
                 OPTION THAT MUST BE FOLLOWED BY NETSPY SMF = NNN  
                 STATEMENT. PLEASE CODE THE MISSING STATEMENT  
                 BEFORE THIS STATEMENT: %LINE

TYPE:           Error

REASON:          The NETSPY SMF = nnn is not coded to declare the  
                  SMF record number for the NSPY data source that  
                  is used in the DATA SOURCE statement that  
                  preceded it.

ACTION:          Edit prefix.MICS.PARMS(SNTOPS) and specify  
                  NETSPY SMF = nnn before the statement given in  
                  the message text referenced above, or remove the  
                  NSPY option from the preceding DATA SOURCE  
                  statement.

                  Resubmit the prefix.MICS.CNTL(SNTPGEN).

REFERENCES:      Chapter 7 of this guide

**SNT00338**

```
+-----+
| S N T 0 0 3 3 8 |
+-----+
```

TEXT: PREVIOUS DATA SOURCE STATEMENT CONTAINED NTCB  
OPTION THAT MUST BE FOLLOWED BY NETTCP SMF = NNN  
STATEMENT. PLEASE CODE THE MISSING STATEMENT  
BEFORE THIS STATEMENT: %LINE

TYPE: Error

REASON: The NETTCP SMF = nnn is not coded to declare the  
SMF record number for the NTCB data source that  
is used in the DATA SOURCE statement that  
preceded it.

ACTION: Edit prefix.MICS.PARMS(SNTOPS) and specify  
NETTCP SMF = nnn before the statement given in  
the message text referenced above, or remove the  
NTCB option from the preceding DATA SOURCE  
statement.

Resubmit the prefix.MICS.CNTL(SNTPGEN).

REFERENCES: Chapter 7 of this guide

## SNT00339

```
+-----+
| S N T 0 0 3 3 9 |
+-----+
```

TEXT:       ==> SMF RECORD NUMBER ABOVE IS %BIGSMAL .  
              PLEASE CODE A VALID RECORD NUMBER IN THE  
              RANGE 128 TO 255 TO CONTINUE. REFER TO  
              APPENDIX A OF CA MICS NETWORK OPTION GUIDE  
              FOR MORE DETAILS ABOUT THIS MESSAGE.

TYPE:       Error

REASON:     The NETSPY SMF = nnn or NETTCP SMF = nnn  
             statement specified an SMF record number for the  
             NSPY or NTCP data source that is not in the  
             acceptable SMF record number range of 128 to  
             255.

ACTION:     Edit prefix.MICS.PARMS(SNTOPS) and specify a  
             valid value for nnn in the NETSPY SMF = nnn  
             statement or NETTCP SMF = nnn statement.

             Resubmit the prefix.MICS.CNTL(SNTPGEN).

REFERENCES: Chapter 7 of this guide

**SNT00341**

```
+-----+
| S N T 0 0 3 4 1 |
+-----+
```

TEXT:       %DEFTOK MUST APPEAR BEFORE ORGSYSID AND AFTER  
              NETWORK ID STATEMENT.

TYPE:       Error

REASON:     The DEFAULT NETSPY SMF = nnn or DEFAULT NETTCP  
              SMF = nnn did not appear before the ORGSYSID  
              statement. The statement must be coded, if  
              needed, before any ORGSYSID statement is coded  
              and after "NETWORK ID" statement.

ACTION:     Edit prefix.MICS.PARMS(SNTOPS) and specify  
              it as mentioned above.

              Resubmit the prefix.MICS.CNTL(SNTPGEN).

REFERENCES: Chapter 7 of this guide

**SNT00342**

```
+-----+
| S N T 0 0 3 4 2 |
+-----+
```

TEXT:       ABOVE STATEMENT CONTAINS ONE OR MORE INVALID  
              KEYWORD VALUES

TYPE:       Error

REASON:     The DEFAULT NETSPY SMF = nnn or DEFAULT NETTCP  
              SMF = nnn does not contain the word SMF as it is  
              expected in the statement.

ACTION:     Edit prefix.MICS.PARMS(SNTOPS) and correct or  
              provide the word SMF in the statement.

              Resubmit the prefix.MICS.CNTL(SNTPGEN).

REFERENCES: Chapter 7 of this guide

## SNT00343

```
+-----+
| S N T 0 0 3 4 3 |
+-----+
```

TEXT: SMF RECORD TYPE MISSING FROM THE STATEMENT.

TYPE: Error

REASON: The DEFAULT NETSPY SMF = nnn or DEFAULT NETTCP  
SMF = nnn does not contain the SMF record  
number that is required for the statement.

ACTION: Edit prefix.MICS.PARMS(SNTOPS) and code the  
desired SMF record number.

Resubmit the prefix.MICS.CNTL(SNTPGEN).

REFERENCES: Chapter 7 of this guide

**SNT00344**

```
+-----+
| S N T 0 0 3 4 4 |
+-----+
```

TEXT:       %DEFKYWD NUMBER %RECTYPE NOT DEFINED IN  
              SP.MICS.GENLIB(SNTGENIN). TO RESOLVE THIS  
              CONDITION AND FOR MORE INFORMATION ABOUT THIS  
              MESSAGE, PLEASE REFER TO APPENDIX A OF THE  
              NETWORK ANALYZER GUIDE.

TYPE:       Error

REASON:     The DEFAULT NETSPY SMF = nnn or DEFAULT NETTCP  
              SMF = nnn, or DEFAULT IBMTCP SMF = nnn defines  
              the SMF record number that is not defined in the  
              SNTGENIN, or the prefix.MICS.PARMS(DBCONFIG) is  
              not updated.

ACTION:     Edit sharedprefix.MICS.GENLIB(SNTGENIN) and  
              specify the SMF record number displayed in the  
              message text.

Submit sharedprefix.MICS.CNTL(SNTCGEN)

After the SNTCGEN completes successfully, edit  
prefix.MICS.PARMS(JCLGENU) so that it contains  
no keywords (is a blank member) and then submit  
prefix.MICS.CNTL(JCLGENU). Resubmit the  
prefix.MICS.CNTL(SNTPGEN).

REFERENCES: Chapter 7 of this guide

## SNT00345

```
+-----+
| S N T 0 0 3 4 5 |
+-----+
```

TEXT: SMF RECORD NUMBER ABOVE IS %BIGSMAL. PLEASE  
CODE A VALID RECORD NUMBER BETWEEN 128 AND 255

TYPE: Error

REASON: The DEFAULT NETSPY SMF = nnn or DEFAULT NETTCP  
SMF = nnn contains the SMF record number  
that is not in the range of 128 through 255.

OR

The DEFAULT IBMTCP SMF = nnn contains an SMF  
record number that is not 118 or 119. This must  
be 118 or 119. Any other SMF record number is  
not acceptable.

ACTION: The DEFAULT NETSPY SMF = nnn or DEFAULT NETTCP  
SMF = nnn statement specified an SMF record  
number that is not in the acceptable SMF record  
number range of 128 to 255.

OR

The DEFAULT IBMTCP SMF = nnn must specify either  
SMF record number 118 or 119. No other SMF  
record number is acceptable for this statement.

Edit prefix.MICS.PARMS(SNTOPS) and specify a  
valid value for nnn in the statement in error.

Resubmit the prefix.MICS.CNTL(SNTPGEN).

REFERENCES: Chapter 7 of this guide



**SNT00346**

```
+-----+
| S N T 0 0 3 4 6 |
+-----+
```

TEXT: %DEFSTMT - DUPLICATE STATEMENT NOT PERMITTED.

TYPE: Error

REASON: The DEFAULT NETSPY SMF = nnn is coded more than once. Duplicate statements are not allowed by the SNTPGEN process.

ACTION: Remove the duplicate statement in error.

Edit prefix.MICS.PARMS(SNTOPS) and delete the line containing the duplicate statement.

Resubmit the prefix.MICS.CNTL(SNTPGEN).

REFERENCES: Chapter 7 of this guide

**SNT00347**

```
+-----+
| S N T 0 0 3 4 7 |
+-----+
```

TEXT: TIME OFFSET STATEMENT NOT FOUND.

TYPE: Error

REASON: The CA MICS Network Analyzer parameter generation program requires that you provide a TIME OFFSET statement in the SNTOPS parameter. This message is issued when it is absent.

ACTION: Code a valid TIME OFFSET statement in SNTOPS.

REFERENCES: Chapter 7 of this guide

## SNT00350

```
+-----+
| S N T 0 0 3 5 0 |
+-----+
```

TEXT:           PREVIOUS DATA SOURCE STATEMENT CONTAINED TCP  
                 OPTION THAT MUST BE FOLLOWED BY IBMTCP SMF = NNN  
                 STATEMENT. PLEASE CODE THE MISSING STATEMENT  
                 BEFORE THIS STATEMENT: %LINE

TYPE:           Error

REASON:          The IBMTCP SMF = nnn is not coded to declare the  
                  SMF record number for the TCP data source that  
                  is used in the DATA SOURCE statement that  
                  precedes it.

ACTION:          Edit prefix.MICS.PARMS(SNTOPS) and specify  
                  IBMTCP SMF = nnn before the statement given in  
                  the message text referenced above or remove the  
                  TCP option from the preceding DATA SOURCE  
                  statement.

                  Resubmit the prefix.MICS.CNTL(SNTPGEN).

REFERENCES:      Chapter 7 of this guide

**SNT00351**

```
+-----+
| S N T 0 0 3 5 1 |
+-----+
```

TEXT: IBMTCP SMF = NNN STATEMENT FOUND AFTER A DATA SOURCE STATEMENT THAT DID NOT SPECIFY TCP OPTION OR THIS STATEMENT IS DEFINED MULTIPLE TIMES.

TYPE: Error

REASON: The TCP option was not used in the DATA SOURCE statement that preceded the IBMTCP SMF = nnn statement (which is used to declare the SMF record number for the TCP data source). Another reason this message could be seen is that there may be a duplicate IBMTCP SMF = nnn statement.

ACTION: Edit prefix.MICS.PARMS(SNTOPS) and remove the statement in question or specify the TCP option on the preceding DATA SOURCE statement.

Resubmit the prefix.MICS.CNTL(SNTPGEN).

REFERENCES: Chapter 7 of this guide

## SNT00352

```
+-----+
| S N T 0 0 3 5 2 |
+-----+
```

**TEXT:** SMF RECORD NUMBER IS MISSING FROM THE STATEMENT. PLEASE CODE %TOK\_CK13 RECORD NUMBER TO CONTINUE. REFER TO APPENDIX A OF CA MICS RESOURCE MANAGEMENT NETWORK OPTION GUIDE FOR MORE DETAILS ABOUT THIS MESSAGE.

**TYPE:** Error

**REASON:** As indicated in the message text, the IBMTCP SMF parameter requires an SMF record number (118 or 119) that is not found. You must provide this value to avoid further abends.

**ACTION:** Edit prefix.MICS.PARMS(SNTOPS), specify the SMF record number referenced in the error message, and resubmit the prefix.MICS.CNTL(SNTPGEN).

**REFERENCES:** Chapter 7 of this guide

**SNT00353**

```
+-----+
| S N T 0 0 3 5 3 |
+-----+
```

**TEXT:** THE TCP SMF RECORD NUMBER %ITCPRYP DECLARED IS NOT DEFINED IN SP.MICS.GENLIB(SNTGENIN) INPUTSOURCE STATEMENT OR THE SMF RECORD TYPE IS NOT 118 OR 119.

**TYPE:** Error

**REASON:** The SMF record number specified for TCP option with IBMTCP SMF = nnn statement is not defined in the sharedprefix.MICS.GENLIB(SNTGENIN) INPUTSOURCE statement or the record number defined is not 118 or 119. TCP/IP data generated by z/OS Communication Server can be either 118 or 119. Any record number other than 118 or 119 for TCP data source is invalid.

**ACTION:** Edit sharedprefix.MICS.GENLIB(SNTGENIN) and specify the valid SMF record number displayed in the message text if not already defined.

Submit sharedprefix.MICS.CNTL(SNTCGEN)

After the SNTCGEN completes successfully, edit prefix.MICS.PARMS(JCLGENU) so that it contains no keywords (is a blank member) and then submit prefix.MICS.CNTL(JCLGENU).

Resubmit the prefix.MICS.CNTL(SNTPGEN).

**REFERENCES:** Chapter 7 of this guide

## SNT00354

```
+-----+
| S N T 0 0 3 5 4 |
+-----+
```

TEXT:           AT LEAST ONE OF THE FOLLOWING STATEMENTS MUST BE  
                 DEFINED:

                  DEFAULT %DEFSTMT    THAT SETS UP DEFAULT VALUES  
                  %DEFSTMT            OVERRIDE THE DEFAULT  
                  NONE WAS FOUND FOR PREVIOUS ORGSYSID=%ORGSYSID.

TYPE:           Error

REASON:          At least one of the values from the pair DEFAULT  
                  TIME OFFSET n and TIME OFFSET n, or from the  
                  pair DEFAULT DATA SOURCES datasrc1 datasrc2 ...  
                  and DATA SOURCES datasrc1 datasrc2 ... must be  
                  coded. Neither of the required keyword  
                  statements was found.

ACTION:          Code either of the necessary statements in  
                  prefix.MICS.PARMS(SNTOPS).

                  Resubmit the prefix.MICS.CNTL(SNTPGEN).

REFERENCES:      Chapter 7 of this guide

**SNT00361**

```
+-----+
| S N T 0 0 3 6 1 |
+-----+
```

**TEXT:** TCP/IP DATA FOR  
          NETWRKID = SEMNET  
          ORGSYSID = 1X01  
          SMFRTYPE = 118  
          IS FOUND IN THE INPUT STREAM, BUT THIS  
          COMBINATION IS NOT DEFINED IN SNTOPS AND WILL  
          NOT BE PROCESSED.

**TYPE:** Warning

**REASON:** The input data stream contained TCP/IP data for  
the network ID, original SYSID, and SMF record  
type shown in the message. However, this  
combination is not defined in SNTOPS at all, or  
at least not to process TCP/IP data. The data  
is read during the initial processing phase of  
DAY056 and then rejected because it fails the  
selection criteria as defined in SNTOPS.

**ACTION:** If you want to process this data, appropriate  
parameter statements must be put in SNTOPS  
followed by a run of prefix.MICS.CNTL(SNTPGEN);  
or else no action is needed. Otherwise, avoid  
including this TCP/IP data in the input stream  
to improve DAY056 execution time.

**REFERENCES:** Chapter 7 of this guide

## SNT00400

```
+-----+
| S N T 0 0 4 0 0 |
+-----+
```

TEXT: CA MICS SNT COMPONENT EXCEPTION VALUE ANALYZER  
BEGINNING SCAN OF %TIMESPAN FILE %DBFILE

TYPE: Information

REASON: This message is issued at the beginning of the  
daily run of the CA MICS Network Analyzer  
exception processor to provide runtime control.

ACTION: None

REFERENCES: None

## SNT00401

```
+-----+
| S N T 0 0 4 0 1 |
+-----+
```

TEXT: %NUMEXC EXCEPTIONS FOUND IN FILE: %DBFILE

TYPE: Information

REASON: This message is issued at the end of each file  
during the CA MICS Network Analyzer's daily run  
of the exception processor. The purpose of the  
message is to report the number of exception  
conditions found on each file.

ACTION: None

REFERENCES: None



**SNT00402**

```
+-----+
| S N T 0 0 4 0 2 |
+-----+
```

TEXT:       SCAN OF FILE %DBFILE COMPLETED. %SCANCNT RECORDS  
             EXAMINED.

TYPE:       Information

REASON:     This message can be issued either from the daily  
             execution of the CA MICS Network Analyzer's  
             exception routine or the exception value  
             analyzer (EVA) routine. The purpose of the  
             message is to report the total number of  
             observations read for each file.

ACTION:     None

REFERENCES:  None



# Appendix B: DATA DICTIONARY

---

The Data Dictionary is only available at your site, where it has been customized to your configuration and your product change level.

To see the Data Dictionary at your site, follow the instructions under Document Browse in the Document Access guide.