

---

---

# Unicenter

## NetSpy Network Performance Administrator Guide

Version 6.0



**Computer Associates**  
The Software That Manages eBusiness



This documentation and related computer software program (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by Computer Associates International, Inc. ("CA") at any time.

This documentation may not be copied, transferred, reproduced, disclosed or duplicated, in whole or in part, without the prior written consent of CA. This documentation is proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of this documentation for their own internal use, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the confidentiality provisions of the license for the software are permitted to have access to such copies.

This right to print copies is limited to the period during which the license for the product remains in full force and effect. Should the license terminate for any reason, it shall be the user's responsibility to return to CA the reproduced copies or to certify to CA that same have been 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 the end user or any third party for any loss or damage, direct or indirect, from the use of this documentation, including without limitation, lost profits, business interruption, goodwill, or lost data, even if CA is expressly advised of such loss or damage.

The use of any product referenced in this documentation and this documentation is governed by the end user's applicable license agreement.

The manufacturer of this documentation is Computer Associates International, Inc.

Provided with "Restricted Rights" as set forth in 48 C.F.R. Section 12.212, 48 C.F.R. Sections 52.227-19(c)(1) and (2) or DFARS Section 252.227-7013(c)(1)(ii) or applicable successor provisions.

© 2002 Computer Associates International, Inc. (CA)

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.



# Contents

---

## Chapter 1: Defining Initialization Parameters

Tuning NetSpy to Your Requirements .....	1-1
INITPRM File Names and Formats .....	1-1
For First-time Users .....	1-1
Parameter Statement Syntax .....	1-2
Specifying Generic Names .....	1-2
Terminal Prefix and Generic Name .....	1-2
Notation Conventions .....	1-3
INITPRM Parameter Descriptions .....	1-4
ACCSSRTM .....	1-4
ACCTING .....	1-5
ALDESC .....	1-5
ALMAXE .....	1-6
ALROUT .....	1-6
ALTBITVL .....	1-7
ALWRITE .....	1-7
AMAXENT .....	1-7
APPL .....	1-8
APPLNAME .....	1-14
APLTOAPL .....	1-15
AUDITCLS .....	1-15
AUDITDST .....	1-15
BASEITVL .....	1-16
CINCLUDE .....	1-16
CNFGITVL .....	1-17
CONSINTF .....	1-17
DBSTART .....	1-18
DBSTOP .....	1-18
DNSMF .....	1-19
FINCLUDE and FEXCLUDE .....	1-19
FORCEDR .....	1-20

---

GMAXENT .....	1-21
HCUTOFF .....	1-21
HOSTID .....	1-22
HPRDATA .....	1-22
IGNRLOGN .....	1-22
INTERVAL .....	1-23
LANGUAGE .....	1-23
LOGDUMP .....	1-24
LOGSTART .....	1-24
LOGSTOP .....	1-25
LOGTYPE .....	1-25
LOSTDATA .....	1-26
LU62RESP .....	1-26
MAX#NCP .....	1-27
MAX#NRPT .....	1-28
MAXAPPL .....	1-28
MAXCA .....	1-29
MAXFCMD .....	1-29
MAXJOBFF .....	1-30
MAXLU .....	1-30
MAXNCPSZ .....	1-31
MAXNOSA .....	1-32
MAXNOVR .....	1-32
MAXOPER .....	1-33
MAXTCMD .....	1-34
MAXTRACE .....	1-34
MAXTRALL .....	1-35
MAXTRINC .....	1-35
NCPRETRY .....	1-36
NCUTOFF .....	1-36
NETRSP .....	1-37
NEUPERF .....	1-37
NSYNAME .....	1-38
NSYXNAME .....	1-39
NTARGETS .....	1-40
NULLTREC .....	1-41
OPTMOD .....	1-41
PMI .....	1-43
RIFABNRM .....	1-43
RIFNORM .....	1-44
SECURE .....	1-44

---

SMF .....	1-45
SMFSTART .....	1-46
SMFSTOP .....	1-46
SMGRID .....	1-47
SNAMDATA (For Unicenter SNA Manager Option Only) .....	1-47
SNMPAGNT (For Unicenter SNA Manager Option Only) .....	1-48
SNMPHOST .....	1-50
STOP .....	1-52
SYNC .....	1-53
TARGETS .....	1-53
TCPIPMON .....	1-54
TELNETLU .....	1-55
TINCLUDE and TEXCLUDE .....	1-57
TRACE .....	1-58
TRACEALL .....	1-58
TRACEEXEC .....	1-59
TRACEHST .....	1-60
TRACEINC .....	1-60
TRACELN .....	1-61
TRACENET .....	1-61
TRACEUSR .....	1-62
TRANSGRP .....	1-62
TRCBUFNO .....	1-63
TRCSTART .....	1-63
TRCSTOP .....	1-64
USRIDUPD .....	1-64
UTARGETS .....	1-65
VTAMINTF .....	1-66
INITPRM Parameter Quick-Reference .....	1-67

## Chapter 2: Defining Startup Parameters

NetSpy Startup Parameters .....	2-1
COLLECT Statement .....	2-2
COLLECT POLLSTAT Statement .....	2-6
CONNECT Statement .....	2-7
How to Start NetSpy-to-NetSpy Communication .....	2-8
DEFINE Statement .....	2-8
NETACCT Statement .....	2-11
SSMF Statement .....	2-14

---

## Chapter 3: Defining Monitors for General Alerts

Defining General Alert Monitors .....	3-1
ALERTPRM File Names and Formats .....	3-1
Monitor Status Display .....	3-1
Monitor Statement Syntax .....	3-2
VTAM vs. NCP Data .....	3-2
For VTAM Data .....	3-3
For NCP Data .....	3-4
Monitor Statement Operands .....	3-6
Monitor Name .....	3-6
MONITOR Resource Types .....	3-6
MONITOR Threshold Variables .....	3-7
MONITOR Optional Operands .....	3-10

## Chapter 4: Installing the Unicenter Interface (Optional)

Managing Your SNA Resources from a Workstation .....	4-1
CA-Datcom .....	4-1
Establishing Communication with Unicenter .....	4-2
Installing Required Software .....	4-2
Allocating the Database .....	4-3
Updating the Database When Upgrading .....	4-3
Modifying the NetSpy PROC .....	4-4
Specifying IP Addresses .....	4-4
Customizing Settings .....	4-4
Notes on Installing CA-Datcom/AD .....	4-6
Installing CA-Datcom/AD .....	4-6
Specifying Parameters for the Unicenter Interface .....	4-7
Using Cross-Communication to Map Your SNA Configuration .....	4-8
SNMPAGNT Parameter .....	4-8
Mapping Your SNA Configuration in a Multiple Host Environment .....	4-9
Communicating SNA Configuration Information to Unicenter .....	4-9
Defining Historical Data to Unicenter .....	4-10

---

## Chapter 5: Installing the Security Interface

Security Packages .....	5-1
RACF, CA-Top Secret, CA-ACF2 .....	5-1
SECURE Parameter .....	5-1
User ID .....	5-1
Authorization Level .....	5-2
Install the Security Interface .....	5-2
File Contents .....	5-2
Procedure .....	5-2

## Chapter 6: Generating NPA Support for Your NCPs

The BUILD Definition Statement .....	6-1
NPA Definition Statements .....	6-2
Troubleshooting .....	6-4

## Chapter 7: Activating the Unicenter Performance Management Predictor Option

Initialization Parameters .....	7-1
NEUPERF Parameter .....	7-1
JCL for NSYNHIST .....	7-3
Control Statements .....	7-3

## Chapter 8: Installing a Session Manager Interface

Session Managers Supported .....	8-1
How to Install a Session Manager Interface .....	8-2
For CA-TPX Users Only .....	8-2
Test the interface .....	8-3
For CA-Television Users Only .....	8-3

## Chapter 9: Creating and Enabling the NetView Interface

Create a Startup Procedure for NetView .....	9-1
Steps to Enable the Interface .....	9-1
NetView Return Codes .....	9-3

---

## Chapter 10: Log Record Layouts

Log Record Types .....	10-1
SMF Record Header .....	10-2
Type A (Application) Entry .....	10-5
Type B (VTAM Buffer) Entry .....	10-7
Type C (Network Accounting) Entry .....	10-8
Type D (APPN Directory Services) Entry .....	10-12
Type E (MNPS Application Recovery) Entry .....	10-13
Type F (MNPS Coupling Facility Structure) Entry .....	10-13
Type G (UDP Connection) Entry .....	10-13
Type H (Interface) Entry .....	10-14
Type I (TCP Connection) Entry .....	10-15
Type J (Stack) Entry .....	10-16
Type M (MNPS Application) Entry .....	10-18
Generic Type N Entry .....	10-19
Type N (HPR) Entry .....	10-22
Type N (Line, Controller, Terminal) Entry .....	10-23
Type N (NCP Major Node) Entry .....	10-25
Type N (NPSI) Entry .....	10-26
Type N (NTRI) Entry .....	10-28
Type N (TIC3) Entry .....	10-30
Type N (Ethernet Adapter) Entry .....	10-32
Type N (Frame Relay) Entry .....	10-33
Type N (NCP Control Block Information) Entry .....	10-35
Type N (Transmission Priority) Entry .....	10-38
Type P (APPN Topology) Entry .....	10-39
Type R (VTAM RTP) Entry .....	10-40
Type S (Terminal Session) Entry .....	10-41
Type T and U (Terminal) Entries .....	10-43
Type V (Virtual Route) Entry .....	10-45
Type X (General Alert) Entry .....	10-47
Trace Record Layout .....	10-51

## Chapter 11: Converting NCP Records to Type 38 Format

Using the NSYCONV Conversion Utility .....	11-1
NSYCONV Program Statements .....	11-2
Start and Stop Time Parameters .....	11-2
Record Type Parameter .....	11-2
Print Parameter .....	11-3

---

## Chapter 12: Converting Log Records to Type 28 Format

Using the N28CONV Conversion Utility .....	12-1
N28CONV Program Statements .....	12-2
Start and Stop Time Parameters .....	12-2
Record Type Parameter .....	12-3
Print Parameters .....	12-3
Error Parameters .....	12-4
DO Parameter .....	12-5
Record Maps .....	12-6
SMF Record Header Map .....	12-6
Type A (Application) Record Map .....	12-10
Type C (Accounting) Record Map .....	12-13
Type D (APPN Directory Services) .....	12-16
Type E (MNPS Application Recovery) .....	12-18
Type F (CFS) .....	12-18
Type M (MNPS Application) .....	12-18
Type N (NCP Resource) Record Map .....	12-19
Type N (Line, Controller, Terminal) Record Map .....	12-20
Type N (X.25 NPSI) Record Map .....	12-21
Type N (Token-Ring) Record Map .....	12-23
Type N (TIC3) Record Map .....	12-25
Type N (Ethernet Adapter) Record Map .....	12-26
Type N (Frame Relay) Record Map .....	12-27
Type P (APPN Topology) .....	12-28
Type R (VTAM RTP) .....	12-30
Type S (Terminal Session) Record Map .....	12-31
Type T and U (Terminal) Record Map .....	12-35
Type X (General Alert) Record Map .....	12-39

## Chapter 13: Using Database Utilities

Converting Database Records to Log Format .....	13-1
Converting Log Records to Database Format .....	13-2
Purging the Database .....	13-2

## Chapter 14: Installing the APPN Monitor (Optional)

Install the APPN Monitor .....	14-1
--------------------------------	------

---

## Appendix A: System Requirements

Virtual Storage Amounts .....	A-1
Base Storage .....	A-1
Batch Reporting .....	A-1
Collection Enhancements .....	A-2
Dynamic Reconfiguration Storage .....	A-2
Graphic Alerts .....	A-2
NCP Definitions .....	A-3
NCP Statistics .....	A-3
Network Accounting .....	A-5
Gateway Accounting Storage .....	A-5
NetSpy-to-NetSpy, Collection Enhancements, and Alerts .....	A-5
Online Reporting .....	A-5
RPL (Request Parameter List) .....	A-5
Session Control Blocks .....	A-6
General Alerts .....	A-6
Help System .....	A-6
Number of Control Blocks Defined in the NCP .....	A-6
CSA Storage Amounts .....	A-7
Application Statistics .....	A-7
Base Storage .....	A-7
Buffer Statistics .....	A-7
Buffer Trace Blocks .....	A-8
Exception Trace Buffers .....	A-8
Monitoring Commands .....	A-8
SMF Type S Record Buffer .....	A-8
Terminal Statistics .....	A-8
Virtual Route .....	A-9
VTAM Tuning Statistics .....	A-9
Reducing Storage Requirements .....	A-9
Above 16 MB Line .....	A-9
Major Nodes Active .....	A-9
Multiple TCP/IP Stack Storage Amounts .....	A-10
Amount of Data Logged .....	A-10

---

## Appendix B: Answers to Common Questions

How to Handle Abends .....	B-1
Authorizing NetSpy to Run at Your Site .....	B-2
Sharing Log Files .....	B-3
Updating the NETSPY.LOADLIB Data Set .....	B-3
Mapping Line and Cluster Data to NTRI and X.25 Resources .....	B-3
Using the Enhanced Application Monitoring Feature .....	B-6
How PLUs and SLUs Are Displayed .....	B-6
Scenarios .....	B-6
Configuring NetSpy in a Sysplex Environment .....	B-9
Sample JCL Statements .....	B-9
How to Contact Technical Support .....	B-10
Information You Can Provide .....	B-10
Ways to Contact .....	B-10

## Appendix C: Contacting Technical Support

Overview .....	C-1
Diagnostic Procedures .....	C-2
Collecting Diagnostic Data .....	C-3
Interpreting Diagnostic Data .....	C-3
Accessing the Online Client Support System .....	C-4
Requirements for Using StarTCC .....	C-4
StarTCC Security .....	C-4
Accessing StarTCC .....	C-5
Accessing the Product Support Directory Online .....	C-5
CA-TLC: Total License Care .....	C-5
Calling Computer Associates Technical Support .....	C-6
Product Releases and Maintenance .....	C-7
Requesting Enhancements .....	C-7

## Index



# Defining Initialization Parameters

---

Control statements in the INITPRM member pertain to the VTAM applications and terminals that NetSpy will monitor and to the session manager interface. As stated in the installation chapters of the NetSpy *Getting Started* guide, you must tailor the initialization parameters to follow your site's requirements.

## Tuning NetSpy to Your Requirements

The defaults in this chapter should be appropriate for most users. Some options are present to maintain compatibility with previous versions of NetSpy.

### INITPRM File Names and Formats

The initialization parameters are read from the sequential data set identified by the //INITPRM DD statement in the startup procedure. If you have OS/390 or z/OS, and VTAM V3 or higher, all CSA will be above 16 MB in virtual storage.

### For First-time Users

If you are a first-time user of NetSpy, see the sample parameters in member INITPRM of *dsnpref.NYvvv.CNTL*. If you are using CA-TPX or another multiple session manager, you need to specify the parameters described in the chapter, "Installing a Session Manager Interface" in the NetSpy *Getting Started* guide.

## Parameter Statement Syntax

On all control statements, you can include comments on the same line. The comment delimiter is a semicolon (;), which can appear in any column. The semicolon indicates that the remainder of the line is a comment. A semicolon or an asterisk (\*) in column one makes the entire line a comment.

Parameters must be coded in columns 1 through 70. Statements can be continued on succeeding lines. Any nonblank character in column 72 indicates a continuation, which cannot be in the middle of a keyword parameter and its value.

### Specifying Generic Names

Before you begin to tailor the NetSpy parameters, you should understand how NetSpy interprets a *generic name*. You can specify one or more asterisks (\*) or a question mark (?) as part of a generic name, as follows:

- One asterisk by itself represents up to eight letters or numbers; for example, CINCLUDE=\* selects all known resources.
- One asterisk at the end of the name represents up to seven letters or numbers, for example, CINCLUDE=C\* is the same as C?, C??. C???, C????, and so on.
- One asterisk in the middle of the name represents only one letter or number, for example, CINCLUDE=C\*2 matches C02, C12, C32, C42, and so on.
- One question mark in any position in the name represents only one letter or number, for example, CINCLUDE=C? matches only C, C1, C2, C3, and so on.

**Note:** The question mark is not valid in generic names used on the DEFINE, SSMF, and COLLECT statements in the STARTPRM file.

### Terminal Prefix and Generic Name

Several parameters allow you to enter a terminal prefix or a generic name; however, they are not the same thing. A terminal prefix will match any terminal whose name begins with the characters specified in the prefix. For example, if you have a group of terminals whose names all begin with AB, their terminal prefix would be AB. However, the generic name for this same group would be AB\*.

## Notation Conventions

This manual uses the following notation when describing the syntax of parameter statements.

<b>UPPERCASE</b>	Keywords in all uppercase must be entered exactly as shown.
<b>italics</b>	Italics indicate a variable. You must supply a value for each variable.
<b>[ ]</b>	Brackets indicate the keyword is optional. (Do not insert brackets in the statement.)
<b>{ }</b>	Braces indicate mutually exclusive required operands. You must choose one.
<b> </b>	A vertical bar means you must choose between mutually exclusive values.

## INITPRM Parameter Descriptions

An explanation of the parameters in the INITPRM file follows. Additional information can be found in the section [INITPRM Parameter Quick-Reference](#) in this chapter.

The parameters listed on the following pages are in *alphabetical order*.

### ACCSRTM

This statement tells NetSpy to collect TCPAccess Telnet server session information that relates to a TCP/IP connection.

ACCSRTM=*subsystem*

<b>Subsystem Values</b>	<b>Explanation</b>
<i>subsystem</i>	The subsystem ID associated with a TCPAccess Telnet Server. The subsystem ID must not exceed four characters in length.
<b>Default:</b>	None.

#### **Notes:**

1. NetSpy supports only one TCPAccess Telnet Server RTM even though multiple TCPAccess Telnet Server RTM regions can be started on the same host.
2. The NetSpy VTAM interface must be running, VTAMINTF=YES.
3. You must code at least one TELNETLU statement where ACCESS=YES and one APPL statement where TNMON=YES.

## ACCTING

This statement specifies whether or not this NetSpy is able to receive network session accounting or gateway accounting data from the NCP.

ACCTING=*option*

<b>Option Values</b>	<b>Explanation</b>
----------------------	--------------------

YES	Enables this NetSpy to receive accounting data from the NCP.
-----	--

NO	Disables this NetSpy from receiving accounting data from the NCP.
----	---

<b>Default:</b>	ACCTING=NO
-----------------	------------

**Note:** ACCTING=YES does not start NCP network accounting; it only indicates the NetSpy that is to receive accounting data.

## ALDESC

This statement specifies the descriptor codes used when alerts are issued to the console via WTORs. Refer to IBM's *MVS Routing and Descriptor Codes* for an explanation of specific descriptor codes.

ALDESC=*n, n, n . . . n*

<b>n Values</b>	<b>Explanation</b>
-----------------	--------------------

<i>number</i>	A number from 1 to 16 (inclusive).
---------------	------------------------------------

<b>Default:</b>	None
-----------------	------

## ALMAXE

This statement tells NetSpy how many alerts to queue to the global and/or user alert display. See the *NetSpy User Guide* for a description of global and user alert monitors.

**Note:** For NetSpy 5.0 and above, this statement is ignored, since the alert facility is enhanced to indicate when an alert is relieved (“duplicate” alerts are no longer issued). All alerts that have *not* been relieved will continue to be displayed on the terminal. This statement may be removed in a later NetSpy version.

ALMAXE=*nn*

<b>nn Values</b>	<b>Explanation</b>
<i>Number</i>	The number of alerts that you can view on the Global or User Alert Status Display.
<b>Minimum:</b>	ALMAXE=11
<b>Default:</b>	ALMAXE=50

## ALROUT

This statement specifies the routing codes used when alerts are issued to the console via WTORs. Refer to IBM’s *MVS Routing and Descriptor Codes* for an explanation of specific descriptor codes.

ALROUT=*n, n, n, . . . n*

<b>n Values</b>	<b>Explanation</b>
<i>number</i>	A number from 1 to 16 (inclusive).
<b>Default:</b>	ALROUT=8

## ALTBITVL

This statement tells the NetSpy alert subtask how often to schedule alert monitoring activities.

*ALTBITVL= interval length*

<b>Interval length Values</b>	<b>Explanation</b>
<i>number</i>	The number of seconds in the interval.
<b>Minimum:</b>	ALTBITVL=10
<b>Default:</b>	ALTBITVL=30

**Note:** This parameter is totally independent from the BASEITVL parameter; ALTBITVL only applies to general alerts.

## ALWRITE

This statement specifies when alerts are logged.

*ALWRITE=option*

<b>Option Values</b>	<b>Explanation</b>
INTERVAL	Alerts are written at the end of the interval in which they occur.
FULL	Alerts are written after the logging I/O buffer is full.
<b>Default:</b>	ALWRITE=INTERVAL

## AMAXENT

This statement specifies the number of alert monitors that you can create through both MONITOR statements in the ALERTPRM member or file and the Define Monitors option on the Alerts System Selection Menu.

*AMAXENT=n*

<b>n Values</b>	<b>Explanation</b>
<i>number</i>	Any number.
<b>Default:</b>	AMAXENT=100

## APPL

This statement specifies the characteristics of the applications to be monitored, including the name of the application and several optional parameters. You can include up to 200 APPL statements, and you must include at least one for NetSpy's VTAM interface to be activated.

**Note:** Be sure to place the APPL statement in your INITPRM file *after* any statements that you want to apply to the application, such as TRACELEN or TRACENET.

```
APPL=name [TARGET=objective] [FORCEDR=percentage]  
          [MAXLU=number] [ALIAS=subapplication]  
          [SMANAGER=session manager name] [EOT=mode]  
          [HCUTOFF=response time] [TRACEHST=threshold]  
          [TRACEALL=option] [TRACENET=threshold]  
          [TRLENGTH=number] [TRACEUSR=threshold]  
          [TRSTARTT=time] [TRSTOPT=time]  
          [TNMON=option]
```

APPL= Values	Explanation
<i>Applname</i>	The real network name for this application. All APPL statements must contain real network names when APPLNAME=NETNAME is specified.
<i>acbname(n)</i>	The ACBNAME of the application, which might be different from the application network name. Use <i>acbname</i> when APPLNAME=NETNAME is not specified.  Specify the number of subapplications to this particular application with the optional integer ( <i>n</i> ). When a range of subapplications is specified, the integer ( <i>n</i> ) <i>must be equal</i> to the number of subapplications. The main application (for example TSO) is not counted.
<b>Default:</b>	If you do not specify at least one valid APPL statement, NetSpy's VTAM interface will not be activated.

TARGET= Values	Explanation
<i>t1,t2,t3,t4</i>	The TARGET parameter defines the four service level target objectives. These values are in tenths of a second. (For example, 50 = 5.0 seconds.) With this parameter, you can specify response time ranges, and then NetSpy will count the transactions that fall within those ranges.
<b>Default:</b>	If you do not specify the target objectives, NetSpy will not collect target data.

**FORCEDR= Values***xxx***Explanation**

The percentage, ranging from 10 to 100, of transactions for which NetSpy will force a definite response. This statement is needed for all applications that normally run non-definite response and for which a network response time is desired. The recommended value is 100.

**Note:** Using this parameter creates no application overhead and very minimal line traffic overhead.

If you are using the FORCEDR parameter with applications accessed by 4700 or 8100 type terminals, the FEXCLUDE parameter can be used to avoid exercising this feature with these types of terminals. Remember that NetSpy *automatically* excludes the 4700 and 8100 type terminals from FORCEDR *unless* they are emulating a 3270 or a non-4700 or non-8100 type device.

**Default:**

If you do not specify FORCEDR, definite responses are not forced.

**MAXLU= Values***number***Explanation**

The maximum number of sessions that can be monitored concurrently for this particular application. If you specify too large a number, other applications might not appear in your statistics. MAXLU per application is a subset of the global MAXLU statement.

**Minimum:**

MAXLU=0

**Maximum:**

MAXLU=32767

**Default:**

If you do not specify MAXLU, no limit is imposed on sessions with this application.

**ALIAS= Values***subapplication  
generic name***Explanation**

Should be specified only for applications having subapplications with which the real sessions are established. Examples include TSO and NCCF. ALIAS specifies a generic name that all of the subapplications match. For example, ALIAS=LATSO\*\*\* when the subapplications are of the form LATSO\*\*\*.

**Default:**

None.

**Notes:**

1. Make sure the alias name you choose is unique to only the application desired. For example, ALIAS=A0IT\*\*\*\* will cause each application that begins with A0IT to be monitored under this APPL.
2. If APPLNAME=NETNAME, the ALIAS parameter must be used to select groups of VTAM applications rather than specifying the number of subapplications on the name.
3. Alias names specified on different APPL statements should never overlap. For example, do not specify ALIAS=TSO1\*\*\*\* and ALIAS=TSO\*\*\*\*\* within the same INITPRM member or file.
4. Make sure the alias name is specific enough to select a set of VTAM applications that all exist within one host (that is, one subarea).

**SMANAGER= Values      Explanation**

**Note:** This parameter is only valid when APPLNAME=NETNAME.

<i>session manager name</i>	The session manager's name, such as TPX. You must use this parameter in the APPL statement describing the session manager itself. When you specify SMANAGER, you cannot define the ALIAS or TARGET parameters for this particular application.
-----------------------------	--

**Default:** If you do not specify SMANAGER, the application is not considered as a session manager.

**Note:** This session manager name is not the application ID or task name of the session manager. The session manager exit chooses the name, which you can obtain from the session manager vendor.

EOT Parameter on the APPL Statement

The following values define the end of transaction mode, which determines when NetSpy will calculate host response times for a particular application. The EOT parameter tells NetSpy what to consider as the final output for a specific application. When the application writes its final output, NetSpy takes a second time-stamp (the first having been taken when the transaction reached VTAM). NetSpy then measures host response time as T2 - T1 (second timestamp minus first timestamp).

<b>EOT= Values</b>	<b>Explanation</b>
RSTKYBD	Use this value if your transactions reset 3270 keyboard terminals. This is the recommended value for all your interactive applications (including CICS, IMS, and TSO).
FSTOUT	Use this value if the first output sent to the terminal ends the transactions (usually for JES and printer applications). NetSpy does not force a definite response for FSTOUT.
LASTOUT	<p>Use this value for interactive applications when reset keyboard is not appropriate; for example, when the keyboard is reset before the transaction terminates, or when your terminals are not a 3270 type. NetSpy will consider the transaction terminated by the last output before either the next user input or a gap of 30 seconds or higher that is detected between outputs.</p> <p>The FORCEDR feature is now supported for applications specifying EOT=LASTOUT</p> <p>When EOT=LASTOUT is specified and tracing is selected, the number of trace buffers required by NetSpy is higher. See the <a href="#">MAXTRACE</a> parameter.</p> <p><b>Note:</b> EOT=LASTOUT is <i>not</i> recommended for IMS. Instead, use the RSTKYBD value explained above.</p>
<b>Default:</b>	EOT=RSTKYBD

<b>HCUTOFF= Values</b>	<b>Explanation</b>
<i>time</i>	The maximum application response time in tenths of seconds. If you specify HCUTOFF both globally and on the APPL statement, NetSpy will use the smaller HCUTOFF value.
<b>Default:</b>	If you do not specify HCUTOFF, NetSpy uses no maximum value as a cutoff for recording application response times.

Tracing Parameters on the APPL Statement      The following parameters, specified on the APPL statement, pertain to NetSpy's optional tracing facilities.

<b>TRACEHST= Values</b>	<b>Explanation</b>
<i>time</i>	The threshold for host response time in tenths of seconds for this particular application. If this threshold is exceeded, exception tracing will be triggered.
<b>Default:</b>	If you do not specify TRACEHST, NetSpy will not trace transactions that exceed host response time thresholds for this application.

<b>TRACEALL= Values</b>	<b>Explanation</b>
YES	Buffer tracing should be activated for this particular application.
NO	Specifies that buffer tracing should not be activated for this particular application.
<b>Default:</b>	TRACEALL=NO

<b>TRACENET= Values</b>	<b>Explanation</b>
<i>time</i>	The threshold for network response time in tenths of seconds for this particular application. If this threshold is exceeded, exception tracing will be triggered.
<b>Default:</b>	If you do not specify TRACENET, NetSpy will not trace transactions that exceed network response time thresholds for this application.

<b>TRLENGTH= Values</b>	<b>Explanation</b>
<i>number</i>	The number of data bytes to be traced for each PIU for this particular application while buffer tracing is active. This parameter affects only buffer tracing.
<b>Default:</b>	TRLENGTH=10 (taken from the TRACELEN parameter)

<b>TRACEUSR= Values</b>	<b>Explanation</b>
<i>time</i>	The threshold for user (host + network) response time in tenths of seconds for this particular application. If this threshold is exceeded, exception tracing will be triggered.
<b>Default:</b>	If you do not specify TRACEUSR, NetSpy will not trace transactions that exceed user response time thresholds for this application.
<b>TRSTART= Values</b>	<b>Explanation</b>
<i>hh:mm:ss or hh:mm</i>	The hour, minute, and second that buffer tracing is to be activated for this particular application.
<b>Default:</b>	TRSTARTT=00:00
<b>TRSTOPT= Values</b>	<b>Explanation</b>
<i>hh:mm:ss or hh:mm</i>	The hour, minute, and second that buffer tracing is to be stopped for this particular application.
<b>Default:</b>	The buffer trace will not be deactivated if this parameter is not specified.
<b>TNMON= Values</b>	<b>Explanation</b>
YES	For applications defined with FORCEDR, NetSpy will force a definite response for Telnet server sessions when the LU name matches the name provided on a TELNETLU statement with FORCEDR other than NO coded. If a Telnet protocol is specified on the TELNETLU statement, the protocol must also match.  For TCPaccess Telnet server sessions, this value must be coded to identify the Telnet protocol.
NO	NetSpy will not force a definite response for Telnet server sessions or identify a TCPaccess Telnet server session's Telnet protocol.
<b>Default:</b>	TNMON=NO

**Note:** If you coded an ACCSSRTM statement, you must code at least one APPL statement where TNMON=YES.

Example of APPL

The following example requests that buffer tracing be activated for application CICSPROD at 08:00 and stopped at 15:00. A maximum of 300 data bytes will be traced for each PIU. NetSpy will force a definite response for all (100%) of the transactions. Response time ranges for the target data are 1, 3, 5, and 10 seconds.

```
APPL=CICSPROD TARGET=10,30,50,100      *
FORCEDR=100                            *
TRACEALL=YES                            *
TRSTARTT=08:00:00 TRSTOPT=15:00       *
TRLENGTH=300
```

## APPLNAME

This statement specifies that all application names in all APPL statements are real network names.

```
APPLNAME=NETNAME
```

The format is: APPLNAME=NETNAME

The APPLNAME=NETNAME statement must appear in the INITPRM member before any APPL statements. Using this statement prevents the loss of VTAM statistics for an application when its major nodes are reactivated. When using the APPLNAME=NETNAME statement, you cannot have ranges in the APPL statement. Use the ALIAS parameter instead, as in this example:

```
APPL=LATSO ALIAS=LATSO***
```

rather than:

```
APPL=TSO(50)
```

If monitoring LU 6.2 sessions, you must specify APPLNAME=NETNAME.

**Default:** If APPLNAME=NETNAME is not specified, the default ACBNAMEs are assumed.

## APLTOAPL

This statement specifies which application-to-application sessions should be monitored.

APLTOAPL=*option*

<b>Option Values</b>	<b>Explanation</b>
NORMAL	Tells NetSpy only to monitor sessions where the primary logical unit is an application defined by the APPL statement.
ENHANCED	Tells NetSpy to monitor all sessions with an application defined by the APPL statement regardless of whether the application is the primary or secondary logical unit. If you use this option, you must also specify the statement APPLNAME=NETNAME.
<b>Default:</b>	APLTOAPL=ENHANCED

## AUDITCLS

This statement tells NetSpy which sysout class to use for a spun SYSOUT audit data set. It is required for the SWITCH command to be effective if the audit log is written to SYSOUT.

AUDITCLS = *sysout class*

<b>Sysout Class Value</b>	<b>Explanation</b>
A-Z, 0-9	A one character SYSOUT class
<b>Default:</b>	None.

## AUDITDST

This statement tells NetSpy which destination to use for a spun SYSOUT audit data set.

AUDITDST = *destination*

<b>Destination Value</b>	<b>Explanation</b>
1-8 character destination	Any valid destination defined to the operating system
<b>Default:</b>	None.

## BASEITVL

This statement tells NetSpy how often to schedule time-dependent activities, such as the option of automatically refreshing NetSpy's 3270 displays.

BASEITVL=*time*

Interval Length Values	Explanation
------------------------	-------------

<i>time</i>	The number of seconds in the interval.
-------------	--

<b>Minimum:</b>	BASEITVL=10
-----------------	-------------

<b>Default:</b>	BASEITVL=30
-----------------	-------------

**Notes:**

1. Normally, you should specify a value below 60. If you are running NetSpy's NCP interface, you can prevent unnecessary NCP activity by specifying a value between 30 and 60.
2. The BASEITVL value should divide evenly into the INTERVAL value.

## CINCLUDE

This optional statement specifies which directly attached resources to monitor for VTAM I/O tuning statistics (TNSTATs).

CINCLUDE=*resourcenames*

resourcenames Values	Explanation
----------------------	-------------

<i>resourcenames</i>	The specific or generic resource names to include in TNSTATS display. For example, AE0-L, N059*, L2808, CN4E*, LPU1*.
----------------------	---

<b>Default:</b>	CINCLUDE statements are optional; if no CINCLUDE statements are specified in INITPRM, CINCLUDE defaults to all resources (*).
-----------------	---

**Notes:**

1. More than one resource name can be specified per statement, but commas or blanks must separate them.
2. If you are including an NCP, the *resourcename* specified must be the link station name, *not* the actual NCP name.
3. More than one CINCLUDE statement can be specified in the INITPRM.
4. The number of resources must not exceed the MAXCA value.

## CNFGITVL

This statement specifies how often the SNMP agent (NetSpy) should refresh the configuration map of SNA resources.

CNFGITVL=*interval*

<b>Interval Values</b>	<b>Explanation</b>
<i>n</i>	The number of seconds in the interval.
<b>Minimum:</b>	CNFGITVL=30
<b>Maximum:</b>	CNFGITVL=3600
<b>Default:</b>	CNFGITVL=180

## CONSINTF

This statement defines whether NetSpy commands can be issued from the OS/390 and z/OS system console.

CONSINTF=YES/NO

<b>CONSINTF Values:</b>	<b>Explanation</b>
YES	Indicates the user will be allowed to issue NetSpy commands from the OS/390 and z/OS system console.
NO	Indicates the user will not be allowed to issue NetSpy commands from the OS/390 and z/OS system console.
<b>Default:</b>	NO

## DBSTART

This optional statement tells NetSpy when to start logging to the NetSpy Datacom Database.

DBSTART= *time*

<b>Time Values</b>	<b>Explanation</b>
<i>hh:mm:ss</i> or <i>hh:mm</i>	The hour, minute, and second at which logging is to start.
<b>Default:</b>	If DBSTART is not specified, logging to the Database will not be activated.

### Notes:

1. If you specify DBSTART=00:00:00 and DBSTOP=24:00:00 logging to the Database will never stop.
2. This statement is only valid for OS/390 and z/OS.

## DBSTOP

This optional statement tells NetSpy when to stop logging to the NetSpy Datacom Database. It is meaningless unless the DBSTART statement is specified.

DBSTOP= *time*

<b>Time Values</b>	<b>Explanation</b>
<i>hh:mm:ss</i> or <i>hh:mm</i>	The hour, minute, and second at which logging is to stop.
<b>Default:</b>	DBSTOP=24:00:00 which causes NetSpy to stop logging at midnight.

### Notes:

1. If you specify DBSTART=00:00:00 and DBSTOP=24:00:00 logging to the Database will never stop.
2. This statement is only valid for OS/390 and z/OS.

## DNSMF

This statement specifies whether or not the DN command starts data collection for a resource.

DNSMF=*option*

<b>Option Values</b>	<b>Explanation</b>
YES	Enables automatic starting of resource data collection (if not already started) when the DN command is issued.
NO	Disables automatic starting of resource data collection for a resource (if data is not already being collected) when the DN command is issued.
<b>Default:</b>	DNSMF=NO

## FINCLUDE and FEXCLUDE

This statement is optional and tells NetSpy the prefixes of terminal names for which you want to allow (FINCLUDE) or disallow (FEXCLUDE) the FORCEDR feature.

FINCLUDE=*terminal name prefix*

FEXCLUDE=*terminal name prefix*

<b>FINCLUDE terminal name prefix Values</b>	<b>Explanation</b>
<i>term prefix 1, term prefix 2, term prefix 3, . . .</i>	The terminal name prefixes for which NetSpy is to allow the FORCEDR feature, up to 2,000. NetSpy allows this feature to be used only for terminals having names with prefixes that match the one in FINCLUDE. Also, the application definition must specify FORCEDR, and the two output criteria listed under the FORCEDR statement (see <a href="#">FORCEDR</a> parameter) must be met.
<b>FEXCLUDE terminal name prefix Values</b>	
<i>term prefix 1, term prefix 2, term prefix 3, . . .</i>	The terminal name prefixes for which NetSpy is to disallow the FORCEDR feature, up to 2,000. NetSpy will not use this feature for those terminals having names with prefixes that match the ones in FEXCLUDE.
<b>Default:</b>	If you do not specify FINCLUDE or FEXCLUDE, NetSpy will not treat any terminals specially. All terminals will be considered for FORCEDR if the application specifies it.

**Notes:**

1. Use only *one* type of statement, either FINCLUDE or FEXCLUDE, but not both. FINCLUDE/FEXCLUDE statements cannot be continued to subsequent lines. You can, however, repeat either statement as often as required.
2. If more than the default number of prefixes is listed in FINCLUDE or FEXCLUDE statements (100), you *must* specify the MAXFCMD statement before the FINCLUDE or FEXCLUDE statements in the INITPRM file.
3. You can use FEXCLUDE to disallow FORCEDR on all 4700 or 8100 type terminals. Remember that NetSpy *automatically* excludes the 4700 and 8100 type terminals *unless* they are emulating a 3270, a non-4700, or a non-8100 type device.
4. You can dynamically alter FINCLUDE/FEXCLUDE tables with the SFDR/PFDR commands accessible through NetSpy's Operator Menu.

## FORCEDR

This statement tells NetSpy whether to force a definite response on selected outputs sent by applications you specify. You should indicate the percentage of application transactions you want treated this way on the FORCEDR parameter of the APPL statement (see [FORCEDR= Values](#)).

FORCEDR=*option*

<b>Option Values</b>	<b>Explanation</b>
YES	NetSpy will force the specified definite response.
NO	NetSpy will not force a definite response.
<b>Default:</b>	FORCEDR=NO

**Note:** NetSpy further selects output for forced definite response according to the following criteria:

- The output must terminate the transaction as defined by the EOT parameter in the APPL definition input statement
- The output must follow the 3270 protocol

You can dynamically activate or inactivate this feature through the FORCEDR ACT/INACT command entered on a 3270 screen (as described in the *NetSpy User Guide*).

## GMAXENT

This statement tells NetSpy the maximum number of resources that can be included in a graph produced with the graphic alerts feature.

GMAXENT=*n*

<b><i>n</i> Values</b>	<b>Explanation</b>
<i>number</i>	The maximum number of resources that can be included in a graph.
<b>Default:</b>	GMAXENT=100

**Note:** Keep in mind that if, for example, you set the GMAXENT statement to 100, the alert displays will list data from a random 100 resources, rather than the 100 worst or best resources. Therefore, GMAXENT should be greater than or equal to the number of resources of a particular type.

For example, if you are graphing LU response times, you should set GMAXENT greater than or equal to the number of LUs that NetSpy can monitor (MAXLU).

## HCUTOFF

This statement tells NetSpy the maximum value for host response time, in tenths of seconds, to record. Transactions that exceed this value will have their host response time reported as the cutoff value. HCUTOFF prevents an exceptionally large host time from skewing the average host time for the application or terminal. If you specify HCUTOFF both globally and on the APPL statement, NetSpy will use the smaller HCUTOFF value.

HCUTOFF=*response time*

<b>Response Time Values</b>	<b>Explanation</b>
<i>time</i>	The maximum host response time in tenths of seconds.
<b>Default:</b>	If you do not specify HCUTOFF, NetSpy uses no maximum value as a cutoff for recording host response times.

## HOSTID

This statement tells NetSpy the alternate ID to use in place of the SMF system ID.

HOSTID=*id*

<b>Id Values</b>	<b>Explanation</b>
<i>id</i>	An alternate ID to the SMF system ID. It can be from one to four characters in length. The first character must be an alphabetic or national character; the remaining characters can be alphanumeric or national.
<b>Default:</b>	HOSTID=SMF <i>system ID</i>

## HPRDATA

This statement tells NetSpy whether to log interval records for High Performance Routing (HPR) data. HPR is an addition to the NCP that enhances data routing performance and session reliability.

HPRDATA=*option*

<b>Option Values</b>	<b>Explanation</b>
YES	The HPR records are to be logged.
NO	The HPR records are not to be logged.
<b>Default:</b>	HPRDATA=NO

## IGNRLOGN

This statement tells NetSpy whether or not to measure the response time from the establishment of a session to the first output.

IGNRLOGN=*option*

<b>Option Values</b>	<b>Explanation</b>
NO	NetSpy should measure the response time from session establishment to first output.
YES	NetSpy should not measure the response time from session establishment to first output. Using this option eliminates the problem of printers skewing the response time statistics.
<b>Default:</b>	IGNRLOGN=YES

## INTERVAL

This statement tells NetSpy how often to reinitialize its statistics and write records to SMF and/or log files if requested.

INTERVAL=*interval length*

<b>Interval Length Values</b>	<b>Explanation</b>
<i>minutes</i>	The number of minutes in the interval. A large value might tend to mask aberrations; a small value will use more disk space and CPU time.
<b>Minimum:</b>	INTERVAL=1
<b>Default:</b>	INTERVAL=15

**Note:** The BASEITVL value should divide evenly into the INTERVAL value.

## LANGUAGE

This statement tells NetSpy the language in which the online help facility is presented.

LANGUAGE=*language code*

<b>Language Code Values</b>	<b>Explanation</b>
EU	United States English
EJ	Upper case English for DBCS (Double Byte Character Set) terminals
NA	Disables HELP Panels
<b>Default:</b>	LANGUAGE=EU

## LOGDUMP

This optional statement tells NetSpy whether to dump a Log file before switching to it and overwriting the existing data. It is meaningless unless the LOGSTART statement is specified.

LOGDUMP=*option*

<b>Option Values</b>	<b>Explanation</b>
YES	A log file should be dumped before reusing it. If YES is specified, the user should have allocated a LOGDUMP file large enough to contain all data to be logged by NetSpy during each run. Maintaining this file is your responsibility.  In the event that a LOGDUMP file becomes full, logging will continue, but log files will no longer be dumped before they are reused.
NO	A log file should not be dumped before reusing it.
<b>Default:</b>	LOGDUMP=NO

## LOGSTART

This statement tells NetSpy when to start logging to the Log.

LOGSTART=*time*

<b>Time Values</b>	<b>Explanation</b>
<i>hh:mm:ss</i> or <i>hh:mm</i>	The hour, minute, and second at which logging is to start.
<b>Default:</b>	If LOGSTART is not specified, logging to the Log will not be activated.

**Note:** If you specify LOGSTART=00:00:00 and LOGSTOP=24:00:00, logging to the Log will never stop.

## LOGSTOP

This optional statement tells NetSpy when to stop logging to the Log. It is meaningless unless the LOGSTART statement is specified.

LOGSTOP=*time*

<b>Time Values</b>	<b>Explanation</b>
<i>hh:mm:ss</i> or <i>hh:mm</i>	The hour, minute, and second at which logging is to stop.
<b>Default:</b>	LOGSTOP=24:00:00, which causes NetSpy to stop logging at midnight.

**Note:** If you specify LOGSTART=00:00:00 and LOGSTOP=24:00:00, logging to the Log will never stop.

## LOGTYPE

This optional statement tells NetSpy what number to use in identifying its log records. The LOGTYPE parameter allows users to merge the log data with SMF records and not have conflict with the record identifier.

NetSpy will report on data matching the *current* LOGTYPE. It will not report on previous data matching a *different* LOGTYPE.

LOGTYPE=*record number*

<b>Record number Values</b>	<b>Explanation</b>
0 - 255, inclusive	The record number that NetSpy uses in the records it writes at the end of each interval.
<b>Default:</b>	Is taken from the SMF number parameter. NetSpy will log to the Log and the database, depending on the destinations specified, even if LOGTYPE=0.

## LOSTDATA

This statement enables warning messages concerning control block overflow to be produced whenever specified or whenever defaulted values of the following control blocks are exceeded:

MAX#NCP	MAXLU	MAXAPPL
MAXNOSA	MAXCA	MAXNOVR
MAXJOBFF		

LOSTDATA=*option*

<b>Option Values</b>	<b>Explanation</b>
INTERVAL	If control block overflow occurs during an interval, a message is issued at the end of that interval.
EVERYINT	Once the control block has overflowed, a message is issued at the end of every interval until shutdown.
ONCEONLY	Even though a control block may overflow multiple times during the entire NetSpy run, only one message is issued at the first overflow.
<b>Default:</b>	LOSTDATA=ONCEONLY

## LU62RESP

This statement specifies whether or not response times should be collected for sessions identified as LU 6.2 sessions. If you select the YES option, response times may not be accurate if the LU 6.2 session is processing multiple transactions concurrently or if the primary LU initiates transactions. Selecting the NO option will prevent these LU 6.2 response times from skewing application statistics or summarized terminal reports.

LU62RESP=*option*

<b>Option Values</b>	<b>Explanation</b>
YES	NetSpy will collect response times for LU 6.2 sessions (using the "normal" method, explained below).
NO	NetSpy will not collect response times for LU 6.2 sessions.

<b>Option Values</b>	<b>Explanation</b>
AUTO	NetSpy will collect response times for LU 6.2 sessions and determine automatically which of the following methods of measuring response time to use: <ul style="list-style-type: none"> <li>■ The “normal” method uses the “allocate (attach) and deallocate” protocol to measure response times.</li> <li>■ For LU 6.2 sessions that do not follow the normal protocol, NetSpy measures response times with each “change of direction.”</li> </ul> <p>LU62RESP=AUTO is the recommended value.</p>
<b>Default:</b>	LU62RESP=YES

**Notes:**

1. When you specify LU62RESP=NO, response times will be shown as “N/A.”
2. Network response times are not based on definite response. NetSpy will not force a definite response for LU 6.2 sessions.

**MAX#NCP**

This statement specifies the maximum number of NCPs that may be defined to NetSpy.

**Note:** This parameter may also be written as MAXNONCP or MAXNCPNO.

MAX#NCP=*number*

<b>Number Values</b>	<b>Explanation</b>
<i>number</i>	Maximum number of NCPs defined to NetSpy.
<b>Minimum:</b>	MAX#NCP=0
<b>Maximum:</b>	Limited by the size of the region.
<b>Default:</b>	MAX#NCP=10

**Note:** If your NCPs are very large, you may need to specify a higher value for your installation. NetSpy allocates 55K of private storage at startup time for every increment in MAX#NCP.

## MAX#NRPT

This statement limits the number of graphs that NetSpy will maintain while viewing an online report sent from another NetSpy. It limits the amount of virtual storage used by the online report.

**Note:** This parameter may also be written as MAXNONRPT.

*MAX#NRPT=number*

<b>Number Values</b>	<b>Explanation</b>
<i>number</i>	Maximum number of graphs NetSpy will maintain in virtual storage while viewing an online report sent from another NetSpy.
<b>Minimum:</b>	MAX#NRPT=10
<b>Maximum:</b>	MAX#NRPT=300
<b>Default:</b>	MAX#NRPT=30

## MAXAPPL

This statement defines the maximum number of control blocks used to cross reference applications with multiple network addresses to the application name.

*MAXAPPL=number*

<b>Number Values</b>	<b>Explanation</b>
<i>number</i>	Maximum number of control blocks used to cross reference applications that have multiple network addresses to the application name.
<b>Default:</b>	2 times the number of applications specified in the INITPRM (includes subapplications).  If ACB names are being used, the default is: (# APPLs x 2) + (# subAPPLs x 2)  If APPLNAME=NETNAME is specified, then the default is: (# APPLs x 2) + ((100 x # of ALIAS statements) x 2)

## MAXCA

This statement specifies the maximum number of directly attached resources to monitor for VTAM I/O tuning statistics (TNSTATs). To monitor resources, specify resource names (specific or generic) with CINCLUDE statements.

**Note:** This statement must precede any CINCLUDE statements.

MAXCA=*number*

<b>Number Values</b>	<b>Explanation</b>
<i>number</i>	Maximum number of directly attached resources to monitor.
<b>Minimum:</b>	MAXCA=2
<b>Default:</b>	MAXCA=30

## MAXFCMD

This statement tells NetSpy how many terminal name prefixes you can specify to allow or disallow the FORCEDR feature with the FINCLUDE and FEXCLUDE parameters and/or SFDR and PFDR commands.

MAXFCMD=*number*

<b>Number Values</b>	<b>Explanation</b>
<i>number</i>	Maximum number of terminal name prefixes for FORCEDR feature.
<b>Minimum:</b>	MAXFCMD=2
<b>Default:</b>	MAXFCMD=100

**Notes:**

1. The amount of CSA allocated at startup time is incremented by 17 bytes with each MAXFCMD increment.
2. MAXFCMD must *precede* FINCLUDE and FEXCLUDE in the INITPRM file.

## MAXJOBFF

This statement defines the number of buffers NetSpy allocated that will be used for collecting CRPL and I/O buffer statistics.

MAXJOBFF=*number*

<b>Number Values</b>	<b>Explanation</b>
<i>number</i>	The number of buffers, which must be greater than the maximum number of jobs that open VTAM ACBs.
<b>Minimum:</b>	MAXJOBFF=0
<b>Maximum:</b>	MAXJOBFF=100000
<b>Default:</b>	MAXJOBFF=200

### Notes:

1. Each buffer uses 12 bytes of fixed CSA.
2. If the number of buffers specified in MAXJOBFF is used up, CRPL and I/O buffer statistics will no longer be collected.

## MAXLU

This statement tells NetSpy the total number of concurrent sessions to monitor for all applications.

MAXLU=*number*

<b>Number Values</b>	<b>Explanation</b>
<i>number</i>	<p>The total number of concurrent sessions NetSpy will monitor. This should be at least the number specified in the MAXLU parameter on the APPL statement.</p> <p>If MAXLU is lower than your total number of sessions, NetSpy will monitor <i>only</i> the specified number. However, you will receive incomplete statistics if additional sessions become active.</p> <p>For example, if you specify MAXLU=10 and you have ten terminal users logged on to CICS, you will receive statistics for those applications. If five more users log on to TSO, however, you will not receive statistics for TSO because you will have exceeded your MAXLU.</p> <p>If you are using a session manager, MAXLU must include both the session between the physical terminal and the session manager, and the session between the virtual terminal and the application.</p>

<b>Number Values</b>	<b>Explanation</b>
<b>Minimum:</b>	MAXLU=2
<b>Maximum:</b>	Limited by the size of CSA.
<b>Default:</b>	MAXLU=200

**Note:** The amount of CSA that NetSpy allocates at startup time is incremented by 84 bytes for each MAXLU increment. See the appendix entitled "[System Requirements](#)" for more information on system requirements.

## MAXNCPSZ

This statement tells NetSpy the number of resources (lines, controllers, and terminals) in the largest NCP defined to NetSpy.

MAXNCPSZ=*number*

<b>Number Values</b>	<b>Explanation</b>
<i>number</i>	Number of resources.
<b>Minimum:</b>	MAXNCPSZ=10
<b>Maximum:</b>	Limited by the size of the region.
<b>Default:</b>	MAXNCPSZ=1000

## MAXNOSA

This statement tells NetSpy the maximum number of subareas to monitor to collect virtual route statistics.

MAXNOSA=*number*

<b>Number Values</b>	<b>Explanation</b>
<i>number</i>	Maximum number of subareas that NetSpy is to monitor.
<b>Minimum:</b>	MAXNOSA=0
<b>Maximum:</b>	9999 or the size of CSA, whichever is encountered first.
<b>Default:</b>	MAXNOSA=5

**Note:** The MAXNOSA and MAXNOVR parameters greatly influence the amount of CSA or ECSA that is allocated. NetSpy allocates all the storage during initialization. To maximize storage usage, you should specify the actual number of subareas (MAXNOSA) and virtual routes (MAXNOVR) that you want to monitor. Note that the MAXSUBA parameter in VTAM is the highest subarea number that can be *encountered*, while the MAXNOSA parameter in NetSpy is the maximum number to be *monitored*.

## MAXNOVR

This statement tells NetSpy the maximum number of virtual routes to monitor to determine virtual route delays.

MAXNOVR=*number*

<b>Number Values</b>	<b>Explanation</b>
<i>number</i>	The maximum number of virtual routes that NetSpy is to monitor.
<b>Minimum:</b>	MAXNOVR=1
<b>Maximum:</b>	239976 or the size of CSA, whichever is encountered first. MAXNOVR should never exceed MAXNOSA times 24.
<b>Default:</b>	MAXNOVR=10

**Notes:**

1. You should allow one increment for each combination of destination subarea/virtual route number/transmission priority active on your system. For example, the following combinations are considered to be four separate virtual routes:

```
VR 0   TP 2   Dest. SA 1
VR 0   TP 1   Dest. SA 1
VR 1   TP 2   Dest. SA 1
VR 0   TP 2   Dest. SA 2
```

2. The MAXNOSA and MAXNOVR parameters greatly influence the amount of CSA or ECSA that is allocated. NetSpy allocates all the storage during initialization. To maximize storage usage, you should specify the actual number of subareas (on MAXNOSA) and virtual routes (on MAXNOVR) that you want to monitor.

**MAXOPER**

This statement tells NetSpy how many users you expect to be logged onto NetSpy plus the maximum number of NetSpy-to-NetSpy connections active at any time.

MAXOPER=*number*

<b>Number Values</b>	<b>Explanation</b>
<i>number</i>	Maximum number of users that you expect to be logged onto NetSpy.
<b>Minimum:</b>	MAXOPER=1
<b>Maximum:</b>	Limited by the size of the region.
<b>Default:</b>	MAXOPER=10

**Note:** NetSpy allocates 11K of private storage for every increment in MAXOPER.

## MAXTCMD

This statement tells NetSpy how many terminal name prefixes you can specify to include or exclude terminals from monitoring with the TINCLUDE and TEXCLUDE parameters and/or the SMNR and PMNR commands. See the chapter “Displaying Real-time Data” in the *NetSpy User Guide*.

MAXTCMD=*number*

<b>Number Values</b>	<b>Explanation</b>
<i>number</i>	Maximum number of terminal name prefixes for including or excluding.
<b>Minimum:</b>	MAXTCMD=2
<b>Default:</b>	MAXTCMD=100

### Notes:

1. The amount of CSA allocated at startup time is incremented by 17 bytes with each MAXTCMD increment.
2. MAXTCMD must *precede* TINCLUDE and TEXCLUDE in the INITPRM file.

## MAXTRACE

This statement tells NetSpy the maximum number of transactions to be traced concurrently on an exception basis. The MAXTRACE statement does not affect buffer tracing.

MAXTRACE=*number*

<b>Number Values</b>	<b>Explanation</b>
<i>number</i>	Maximum number of transactions to be traced concurrently. If you specify the MAXTRACE statement with too small a number, transactions might be missed because there will not be enough buffers to handle the number of concurrent transactions.
<b>Minimum:</b>	MAXTRACE=2
<b>Maximum:</b>	Limited by the size of the CSA.
<b>Default:</b>	MAXTRACE=the value of MAXLU divided by 10

**Note:** The default will be too low when tracing transactions for applications that have EOT=LASTOUT specified. In this case, specify the value of MAXLU divided by 3. See the appendix entitled “[System Requirements](#)” for the CSA implications before increasing the value of the MAXTRACE statement.

## MAXTRALL

This statement tells NetSpy the maximum number of terminal names that you can specify to trace all PIUs using the TRACEALL parameter or the STRCA operator command. See the *NetSpy User Guide*.

MAXTRALL=*number*

<b>Number Values</b>	<b>Explanation</b>
<i>number</i>	Maximum number of terminal names.
<b>Minimum:</b>	MAXTRALL=2
<b>Maximum:</b>	Limited by the size of the CSA.
<b>Default:</b>	MAXTRALL=100

## MAXTRINC

This statement tells NetSpy the maximum number of terminal name prefixes that you can specify to include or exclude terminals from tracing with TRACEINC and TRACEEXC, or the STRC and PTRC operator commands. See the *NetSpy User Guide*.

MAXTRINC=*number*

<b>Number Values</b>	<b>Explanation</b>
<i>number</i>	Maximum number of terminal name prefixes.
<b>Minimum:</b>	MAXTRINC=2
<b>Maximum:</b>	Limited by the size of the CSA.
<b>Default:</b>	MAXTRINC=100

## NCPRETRY

This statement sets the global default for the number of times NetSpy will try to acquire an NCP's NPALU session after an NPALU session is lost or an attempt to acquire it has failed. Optionally, you can also specify the length of time between retry attempts. NetSpy uses the global default values only for NCPs for which no REPLY keyword is specified on the DEFINE statement in STARTPRM. You can modify the global defaults after startup by issuing the NCPRETRY command.

`NCPRETRY=number|[(number, time)]`

<b>NCPRETRY Values</b>	<b>Explanation</b>
------------------------	--------------------

<i>number</i>	The number of times NetSpy will try to acquire a lost or failed NCP's NPALU session. Valid values are 0 to 9999.
---------------	--

<i>time</i>	The time between retries in minutes. Valid values are 1 to 9999.
-------------	--

**Default:** `NCPRETRY=(0,NetSpy-interval)`

## NCUTOFF

This statement tells NetSpy the maximum value for network response time, in tenths of seconds, to record. Transactions that exceed this value will have their network response time reported as the cutoff value. NCUTOFF prevents an exceptionally large network time from skewing the average network time for the application or terminal.

`NCUTOFF=response time`

<b>response time Values</b>	<b>Explanation</b>
-----------------------------	--------------------

<i>time</i>	The maximum network response time in tenths of seconds.
-------------	---

**Default:** If you do not specify NCUTOFF, NetSpy uses no maximum value as a cutoff for recording network response times.

## NETRSP

This statement tells NetSpy the type of PIU for which to calculate network response time.

NETRSP=*PIU type*

<b>PIU type Values</b>	<b>Explanation</b>
DATA	NetSpy will calculate network response time for data traffic only. DATA is recommended unless one of the applications you use runs in exception response mode instead of definite response mode, and you are not using the FORCEDR feature.
ALL	NetSpy will calculate network delay for all PIUs, including session control and data flow control.  <b>Note:</b> Specifying NETRSP=ALL may result in inaccurate target distributions for user response times. Use this setting <i>only</i> when you are unable to either use the FORCEDR feature or calculate network response times.
<b>Default:</b>	NETRSP=DATA

## NEUPERF

This statement activates or inactivates the real time interface to the NeuPerformance Advisor for OS/390 and z/OS.

NEUPERF=OFF  
 NEUPERF=ON ENTITY=*entity* SSN=*ssn* FILTWARN=YES|NO ERRLIM=9999999  
 OTHERSYS=INCLUDE|EXCLUDE RECORDS=*recordtypes*

NEUPERF=OFF turns off the real time interface to the NeuPerformance Advisor for OS/390 and z/OS, and is the default.

NEUPERF=ON turns on the interface to the NeuPerformance Advisor for OS/390 and z/OS, which will activate the other parameters.

The following parameters only have meaning if NEUPERF=ON is coded:

<b>Parameter</b>	<b>Explanation</b>
ENTITY= <i>entity</i>	Specifies a one to eight character entity name to be passed to the NeuPerformance Advisor External Data Interface. This value shows up as the <i>session name</i> in NeuPerformance Advisor.  Default is NSYMAIN

Parameter	Explanation
<b>ERRLIM=</b> 99999999	Specifies a one to seven digit maximum number of error messages written to the console that report non-zero return codes from the NeuPerformance Advisor External Data Interface. When the specified number of messages has been written, future errors are not reported.  Default is 10.
<b>FILTWARN=</b> YES or NO	Specifies whether to produce the NSY2103 error message on the console when filtering rejects the data presented to the NeuPerformance Advisor External Data Interface.  Default is NO
<b>OTHERSYS=</b> INCLUDE or EXCLUDE	Specifies which log records collected from other systems are to be passed to the NeuPerformance Advisor External Data Interface. INCLUDE indicates all records will be passed, and EXCLUDE indicates only records created in this NetSpy system will be passed.  The default is INCLUDE.
<b>RECORDS=</b> <i>recordtype</i>	Indicates which record types will be passed to the NeuPerformance Advisor External Data Interface. Specify either ALL, for every record type, or a string of characters separated by commas and enclosed in parenthesis. List the record types as defined in the chapter "Log Record Layouts."  The default is ALL.
<b>SSN=xxxx</b>	Specifies the one to four character subsystem name of the NeuPerformance Advisor External Data Interface.  The default is NEUP.

## NSYNAME

This statement tells NetSpy the VTAM ACBNAME for this NetSpy system.

NSYNAME=*name*

Name Values	Explanation
<i>acbname</i>	The VTAM ACBNAME of the NetSpy system.
<b>Default:</b>	NSYNAME=NETSPY

## NSYXNAME

This statement enables communication between this NetSpy and another NetSpy or NetMaster in your network. The NSYXNAME statement must be specified in the INITPRM member or file of each NetSpy in your network that will be running NetSpy-to-NetSpy or NetSpy-to-NetMaster communications.

See the NetMaster documentation for information on what is required to establish the connection and retrieve NetSpy data.

NSYXNAME=*netspyacb*

Name Values:	Explanation
--------------	-------------

<i>netspyacb</i>	The VTAM ACB name associated with this NetSpy's address space, which is specified on the NetSpy-to-NetSpy APPL statement in your VTAM definitions. (This name must match the ACB name on that same statement.) You must specify a VTAM APPL statement for the NetSpy-to-NetSpy facility in addition to the usual VTAM APPL definition for NetSpy itself. These two APPL definitions must have different ACB and network names.
------------------	--

<b>Default:</b>	This parameter has no default. If you omit it, NetSpy-to-NetSpy or NetSpy-to-NetMaster communication is disabled.
-----------------	---

**Important!** Specify the NSYXNAME parameter in each NetSpy that is to communicate with another NetSpy or NetMaster.

See [How to Start NetSpy-to-NetSpy Communication](#) in the chapter "Defining Startup Parameters" for more information

## NTARGETS

This statement defines the four global network service level objectives (buckets). NTARGETS are targets for use with network response times based on definite response. The NTARGETS statement can be used with the application targets as follows:

If TARGETS = HOST (application targets) and NTARGETS = `____` then you will have four buckets collecting host response times (on an application basis) and four buckets collecting network response times (on a global basis).  
If TARGETS = USER (application targets) and NTARGETS = `____` then you will have four buckets collecting user response times (on an application basis) and four buckets collecting network response times (on a global basis).

NTARGETS=*objective*

### Objective Values Explanation

*t1,t2,t3,t4* These values, specified in tenths of a second, define response time ranges within which NetSpy will count transactions. Because NTARGETS is a system-wide parameter, the ranges specified in it take effect for all sessions in this host.

**Default:** If you do not specify NTARGETS objectives, NetSpy will not collect global network target data.

### Notes:

1. You can specify either the NTARGETS or the UTARGETS parameter, but you cannot specify both.
2. TARGET must be specified on the APPL statement for the application to record targets.
3. The global buckets are written in the SMF and log records only as Type T and U subtype records.

## NULLTREC

This statement tells NetSpy whether to write interval records for sessions (type T records) that have not had any activity to your SMF and log files. Specifying NULLTREC=NO saves disk space and CPU time.

NULLTREC=*option*

<b>Option Values</b>	<b>Explanation</b>
YES	The null type T records are written to the SMF and log files.
NO	The null type T records are not written to the SMF and log files.
<b>Default:</b>	NULLTREC=NO

## OPTMOD

This statement is optional and allows the user to modify the way NetSpy behaves in certain situations. More than one option may be specified per statement, but commas or blanks must separate them.

OPTMOD=*option*

<b>Option Values</b>	<b>Explanation</b>
USELOG1	At startup, begin writing to LOG1 if it is empty.
RPTPRIV	Make online reporting commands privileged.
APPL600	Allow up to 600 applications to be specified.
REMPF12	Disable PF12 and remove it from the displayed list of PF Keys.
LOGOFX	Call NSYUPSWD at logoff (sets R0=4).
HISPEED	Specify high-speed line as the default rather than low speed line for response time corrections. When an LU name is not located in the defined NCP that matches the subarea of the LU, assume the LU is on a high-speed line and do not attempt to correct the response time. This option is intended for users who have token ring or high speed dial-in devices but do not have NPALU sessions with their NCPs.
XNETWK	Search all NCPs for a terminal name regardless of the subarea. This option is used for cross network devices.
FDR4700	Enable FORCEDR for 4700 financial terminals. This option also includes option FDRFOUT.

<b>Option Values</b>	<b>Explanation</b>
FSTOUT5	Terminate host response times for applications with EOT=FSTOUT if the output is less than 5 bytes (PIUs have no data).
IGNRDY	Ignore X'E8' printer ready inputs. NetSpy should not start any transactions when printer ready inputs are received from SNA printers.
FDRFOUT	Allow FORCEDR on devices that only receive formatted outbound requests. This is similar to option FDR4700, except FDR4700 handles devices that both send and receive formatted PIUs.
IGNRADR1	Do not use the FORCEDR option value of application requested definite responses if FORCEDR is not allowed for the device.  <b>Note:</b> Options IGNRADR1 and IGNRNOIC are mutually exclusive.
IGNRNOIC	Ignore the FORCEDR option value of application requested definite responses if FORCEDR is not allowed for the device and the outbound request is not an only-in-chain PIU.  Both these conditions must be met for NetSpy to disregard the application generated definite response.  <b>Note:</b> Options IGNRADR1 and IGNRNOIC are mutually exclusive.
FDRN3270	Allow FDR on non-3270 data streams.
IGNRCLR	Ignore CLEAR and PA2 keys as transaction start.
TRCALLTR	Change the condition under which "exception all" tracing is performed. All transactions will be traced, whether requested or not, and cannot be turned off.
<b>Default</b>	None.

## PMI

This statement tells NetSpy to collect data from the performance monitor interface (PMI), which is available with VTAM 4.3 and above. This interface is required for the collection of APPN and MNPS performance data.

PMI=*option* ACBNAME=*name* EXITNAME=*name*

### PMI Option Values

	Explanation
YES	Activates the PMI when NetSpy starts. Only one NetSpy should have PMI=YES specified per host.
NO	Does not activate the PMI when NetSpy starts. Multiple NetSpys with PMI=NO specified can run on a single host.
<b>Default:</b>	PMI=NO

### ACBNAME Name Values

	Explanation
<i>acbname</i>	The VTAM ACBNAME for the performance monitor interface.
<b>Default:</b>	ACBNAME=NSYPMI

### EXITNAME Name Values

	Explanation
<i>exitname</i>	The load module name of the performance monitor exit routine.
<b>Default:</b>	EXITNAME=NSYPMXIT

## RIFABNRM

This statement is ignored in NetSpy 6.0 because changes to an alert's severity level from normal to abnormal are now reported as soon as the change occurs. The RIFNORM parameter still functions as it has in previous releases.

## RIFNORM

The RIFNORM statement specifies the number of intervals that must pass before NetSpy reports an alert's return to a normal severity level.

You can use the RIFNORM statement to tailor when NetSpy reacts to a change in an alert's condition. The RIFNORM parameter specifies the number of intervals that must pass before NetSpy relieves an alert. If you do not specify this parameter, the default is used.

By default, NetSpy immediately reports an alert if its severity level changes from normal to abnormal *during* the interval. NetSpy reports "relieved" alerts (severity level changed from abnormal to normal) after *two* intervals have passed. This intervening period of time is referred to as the "relaxation interval factor" (RIF).

RIFNORM=*interval*

<b>Interval Values</b>	<b>Explanation</b>
<i>n</i>	The number of intervals.
<b>Default:</b>	RIFNORM=intervals greater than 0

## SECURE

This statement tells NetSpy whether or not to activate the security interface.

SECURE=*option*

<b>Option Values</b>	<b>Explanation</b>
YES	Invokes the security interface at each LOGON request. The NSYUPSWD module must be linked into the NetSpy authorized load library.
NO	NetSpy should bypass all security processing.
<b>Default:</b>	SECURE=NO

## SMF

This statement tells NetSpy the type of records you want written to SMF, your log files, or both at the end of each interval and indicates the SMF record number for NetSpy to use.

*SMF=record number SESSION=option TYPEU=option*

<b>SMF Record Number Values</b>	<b>Explanation</b>
<i>0 and 128-255, inclusive</i>	The record number that NetSpy uses in the records it writes at the end of each interval.
<b>Default:</b>	SMF=0. NetSpy will write no SMF records.

### Notes:

1. To see historical data online, you must collect it in the Log or Database. You can request logging to the Log by specifying the LOGSTART statement. You can request logging to the Database by specifying the DBSTART statement.
2. The timestamp in the SMF record indicates the time the records are written, which occurs at the end of an interval.

<b>SESSION Option Values</b>	<b>Explanation</b>
YES	Session (type S) records will be logged to SMF. In this case, session records are written when the session starts or ends, not at the end of the interval.
NO	Session (type S) records will not be logged to SMF. In this case, you should collect terminal (type U) records.
<b>Default:</b>	SESSION=YES

**Note:** Session (type S) records are logged to SMF and *not* to the Log or Database.

<b>TYPEU Option Values</b>	<b>Explanation</b>
YES	Type U terminal records will be logged to SMF. In this case, you do not need to collect session records (type S).
NO	Type U terminal records will not be logged to SMF.
<b>Default:</b>	TYPEU=NO

**Notes:**

1. Setting TYPEU=YES and SESSION=NO is recommended. See the chapter “[Log Record Layouts](#)” for a description of type S and U records.
2. If both S and U type records are logged, only type U records will be used for historical reporting.

## SMFSTART

This optional statement tells NetSpy when to start logging to SMF. It is meaningless unless the SMF statement is specified with a non-zero record number.

SMFSTART= *time*

<b>Time Values</b>	<b>Explanation</b>
<i>hh:mm</i> or <i>hh:mm:ss</i>	The hour, minute, and second at which logging is to start.
<b>Default:</b>	SMFSTART=00:00:00, which causes NetSpy to start logging immediately at NetSpy startup if the SMF statement is specified with a non-zero record number.

**Note:** If you specify SMFSTART=00:00:00 and SMFSTOP=24:00:00 (or specify neither statement), and the SMF statement with a non-zero record number, logging will never stop.

## SMFSTOP

This optional statement tells NetSpy when to stop logging data to SMF. It is meaningless unless the SMF statement with a non-zero record number is specified.

SMFSTOP= *time*

<b>Time Values</b>	<b>Explanation</b>
<i>hh:mm</i> or <i>hh:mm:ss</i>	The hour, minute, and second at which logging is to stop.
<b>Default:</b>	SMFSTOP=24:00:00 (which causes NetSpy to stop logging at midnight)

**Note:** If you specify SMFSTART=00:00:00 and SMFSTOP=24:00:00 (or specify neither statement), and the SMF statement with a non-zero record number, logging to SMF will never stop.

## SMGRID

This statement tells NetSpy the identifier used by the session manager to inform NetSpy when a user switches sessions. The session manager exit chooses the identifier, which can be obtained from the session manager vendor. TPX and TELEVIEW use the default identifier NETSPY@.

SMGRID=*id*

<b>id value</b>	<b>Explanation</b>
id	Identifier assigned by the session manager (maximum of seven characters).
Default	NETSPY@

## SNAMDATA (For Unicenter SNA Manager Option Only)

This statement specifies the location of NetSpy historical data. The data must be communicated to Unicenter SNA Manager Option for the purpose of displaying reports. You must specify a value other than the default if you have a NetSpy that communicates map information (to SNA Manager Option on the workstation) but stores historical data on another NetSpy.

SNAMDATA=*option*

<b>Option Values</b>	<b>Explanation</b>
LOCAL	The data resides in this NetSpy.
<i>name</i>	The CAICCI system ID for the host where the historical data resides.
<b>Default:</b>	LOCAL

## SNMPAGNT (For Unicenter SNA Manager Option Only)

This statement indicates that NetSpy is to act as a Simple Network Management Protocol (SNMP) subagent and a collector of local SNA configuration data to be registered as variables within a local or remote Management Information Block (MIB). The SNA configuration data is sent to a Unicenter management station.

SNMPAGNT=options

Option Values	Explanation
OSNMPD   name	When specifying a name other than OSNMPD, the name must be resolved by the domain name server, indicated by the SYSTCPD DD card found in the NETSPY JCL.
NO	NetSpy will not collect SNA configuration data to be registered within the local MIB or act as a DPI subagent.
REMOTE	NetSpy will send SNA configuration data to all requesting NetSpys that are acting as a DPI Subagent.
<b>Default:</b>	SNMPAGNT=NO

Code this statement in one of the following three forms:

1. Use the following form when NetSpy is to act as a DPI subagent. When this form of the initialization parameter is coded, NetSpy collects local and remote SNA configuration data and then registers the data in the local MIB.

SNMPAGNT=OSNMPD | name

If you specify a name it must be resolved by the domain name server indicated by the SYSTCPD DD card found in the NetSpy JCL.

NetSpy will communicate with either a TCP/IP or TCPaccess SNMP agent using Distributed Protocol Interface (DPI).

**Note:** A community name of public is assumed.

### For IBM TCP/IP stacks:

The name specified can be either the procedure name of the SNMP agent (depending upon how the agent is started, typically OSNMPD) or the name of the local host TCP/IP stack.

**For TCPaccess stacks:**

- The name specified must be the name of the local host TCP/IP stack.
- You must also relink NetSpy's SNMP DPI module, SNMPPDPI, using TCPaccess libraries.

The sample JCL for relinking NetSpy's SNMPPDPI module for use with TCPaccess can be found in the RELNKDPI member of the *dsnpref.NYvvv.CNTL* library.

- A SYSTCPD DD card must be included in the NetSpy JCL containing the following statements (see SOLVE:TCPaccess Customization Guide and Technical Note 8 SNMP DPI for more information):

```
TCPIPJOBNAME <tcpaccess_jobname>
DNRSSID <tcpaccess_ssid>
TRACEDD SYSPRINT
SOCKDEBUG
```

2. Use the following form when NetSpy is to collect SNA configuration data and send it to another NetSpy that is acting as a DPI SNMP subagent via Netspy-to-NetSpy connection.

```
SNMPAGNT=REMOTE
```

When coding this form, you must also code a NSYXNAME initialization parameter to establish NetSpy to NetSpy communication. SNA configuration data will be sent to all requesting NetSpys that are acting as a DPI subagent. Note that a NetSpy acting as a DPI subagent will send a request for data to every NetSpy that is connected.

3. Use the following form when NetSpy will not collect SNA configuration data to be registered within the local MIB or act as a DPI subagent.

```
SNMPAGNT=NO
```

SNMPAGNT=NO is the default.

**Note:** You must specify VTAMINTF=YES if SNMPAGNT=OSNMPD, SNMPAGNT=*name*, or SNMPAGNT=REMOTE is specified.

## SNMPHOST

**Important!** You *must* have an OMVS security segment associated with the user ID of the NetSpy job or started task. The OMVS security segment may be either an explicit definition or a default definition.

This statement defines a TCP/IP stack to be monitored.

```
SNMPHOST {ADDRESS=ipaddr|NAME=hostname}  
          [PORT=port]  
          [CDELAY=number]  
          [COMMNAME=name]  
          [RECONN=number]  
          [TIMEOUT=number]  
          [TYPE=I|O]  
          [IF=(Y|N, Y|N)]  
          [STACK=(Y|N, Y|N)]  
          [TCP=(Y|N, Y|N)]  
          [UDP=(Y|N, Y|N)]
```

Option Values	Explanation
ADDRESS= <i>ipaddr</i> or NAME= <i>hostname</i>	The name or IP address in dot notation form of the host TCP/IP stack to be monitored. Specify either ADDRESS or NAME, not both.  NetSpy can support a name up to 64-characters long. The specified name must be resolved by the domain name server, which is indicated by the SYSTCPD DD card found in the NETSPY JCL. NetSpy can monitor up to 15 Host TCP/IP stacks at one time.
CDELAY= <i>number</i>	The amount of time, in seconds, that NetSpy will wait between SNMP collection requests. The range can be set from 30 to 999.  <b>Default: 30 seconds</b>
COMMNAME= <i>name</i>	The community name is used by NetSpy on an SNMP collection request. <i>This name is case sensitive</i> and can be up to 32 characters in length.  <b>Default: public</b>
PORT= <i>port</i>	The UDP port number assigned to the SNMP agent.  <b>Default: 161</b>

<b>Option Values</b>	<b>Explanation</b>
RECONN=number	<p>The number of times that NetSpy will attempt to re-connect to the SNMP agent after an unsuccessful connection. Once the connection has failed, NetSpy will only attempt to connection to the SNMP agent on an interval. In other words, after the first failure, NetSpy will terminate monitoring a stack when this number of intervals has been reached without a successful connection.</p> <p>The number of attempts can range from 0 to 255.</p> <p><b>Default:</b> 6 attempts.</p>
TIMEOUT= <i>number</i>	<p>The amount of time, in seconds, that NetSpy will wait for a response from the SNMP agent.</p> <p>The range can be set from 5 to 120 seconds.</p> <p><b>Default:</b> 5 seconds.</p>
TYPE=I or TYPE=O	<p>Currently NetSpy supports two TCPIP stacks. The IBM OS/390 and z/OS stack starting with TCP/IP 3.4 and Computer Associate's TCPaccess 5.2 TCP/IP stack.</p> <p>Enter:</p> <ul style="list-style-type: none"> <li>■ TYPE=I for IBM enterprise as well as some MIBII data.</li> <li>■ TYPE=O for Other, which includes only MIBII data.</li> </ul> <p><b>Default:</b> TYPE=I.</p> <p>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 parenthesis is the collection indicator. Valid values are Y for YES to collect or N for NO not to collect. The second parameter within the parenthesis 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.</p> <p>Valid combinations of these two indicators are: (Y,Y), (Y,N), and (N,N).</p>
IF=(Y N, Y N)	<p>This produces the interface table data.</p> <p><b>Default:</b> IF=(Y,Y), to collect and log interface table data.</p>
STACK=(Y N, Y N)	<p>This produces an overview of the stack, which includes summary information on all 3 groups.</p> <p><b>Default:</b> STACK=(Y,Y), to collect and log stack data.</p>
TCP=(Y N, Y N)	<p>This produces the TCP connection table data.</p> <p><b>Default:</b> TCP=(Y,Y), to collect and log TCP connection table data.</p>

<b>Option Values</b>	<b>Explanation</b>
UDP=(Y N,Y N)	This produces the UDP connection table data.  <b>Default:</b> UDP=(Y,Y), to collect and log UDP connection table data
<b>Default:</b>	SNMPHOST does not have a default option.

**Notes:**

- The TCPIPMON=YES must be coded before the first SNMPHOST initialization parameter.  
  
Including TCPIPMON=YES in the initialization parameters, without any SNMPHOST statements, will allow Host IP stack monitoring to be added after NetSpy is initialized.
- NetSpy can automatically delete any stack defined to NetSpy after the number of contiguously repeated connection attempts equals the RECONN value.

## STOP

This statement indicates how NetSpy will be stopped at the operator's console.

*STOP=option*

<b>Option Values</b>	<b>Explanation</b>
P or F	NetSpy is stopped using the OS/390 and z/OS STOP (abbreviation P) command or OS/390 and z/OS MODIFY (abbreviation F) command. The operator enters one of the following commands to terminate NetSpy:  P NETSPY or F NETSPY,STOP
REPLY	NetSpy is stopped by replying to an outstanding WTOR or message. The operator enters the following command to terminate NetSpy, where <i>n</i> is the number of the outstanding REPLY:  R <i>n</i> ,STOP
<b>Default:</b>	STOP=P

## SYNC

This statement tells NetSpy the time (in minutes and seconds) after the hour at which you want NetSpy to synchronize its logging INTERVAL.

For example, if you specify INTERVAL=15 and SYNC=14:00, then NetSpy will log its records at 14, 29, 44, and 59 minutes past the hour.

*SYNC=synchronization time*

<b>Synchronization Time Values</b>	<b>Explanation</b>
------------------------------------	--------------------

<i>mm:ss (or) ss</i>	The minutes and seconds past the hour on which to synchronize NetSpy logging.
----------------------	---

<b>Default:</b>	SYNC=0 (synchronize on the hour).
-----------------	-----------------------------------

**Note:** The value of the SYNC parameter must be less than the value of the INTERVAL parameter.

## TARGETS

This statement tells NetSpy on a global basis whether to compute targets based on the host response time or the user response time (host+net).

*TARGETS=response time basis*

<b>Response Time Basis Values</b>	<b>Explanation</b>
-----------------------------------	--------------------

HOST	Instructs NetSpy to examine every transaction and update targets accordingly.
------	---

USER	Instructs NetSpy to consider only transactions that use definite response and have a network time when it updates the targets. This is an important consideration if you run NetSpy without the FORCEDR feature or use it less than 100 percent of the time.
------	--

<b>Default:</b>	TARGETS=USER
-----------------	--------------

**Note:** TARGET must be specified on the APPL statement for the application to record targets.

## TCPIPMON

This statement tells NetSpy to establish TCP/IP stack monitoring.

TCPIPMON=*option*

<b>Option Values</b>	<b>Explanation</b>
YES	Indicates TCP/IP monitoring should be initialized.  TCPIPMON=YES must be set prior to encountering any SNMPHOST statements found in the initialization member. All subsequent occurrences of TCPIPMON will be ignored.  <b>Note:</b> When coding TCPIPMON=YES, no SNMPHOST statements are required. TCP/IP monitoring can be established after NetSpy initialization by dynamically adding one or more stacks. Up to 15 stacks may be monitored simultaneously.
NO	Prevents TCP/IP monitoring from occurring.
<b>Default:</b>	TCPIPMON=NO

## TELNETLU

This statement tells NetSpy to force a definite response for Telnet sessions identified by the Logical Unit (LU) name.

```
TELNETLU= luname
          [ACCESS=option]
          [FORCEDR=ALL | (FORCEDR=TN3270 | TN3270E | TN3270ER) | FORCEDR=NO]
```

You can code a maximum of 25 TELNETLU statements.

<b><i>luname</i> Values</b>	<b>Explanation</b>
<i>luname</i>	The name of a Telnet session LU for which you want NetSpy to force a definite response. The value must not exceed eight characters in length.

**Default:** None.

### Notes:

1. You can represent the LU name generically by using an asterisk to specify the range of LU names identified by your IBM TCP/IP profile or your TCPAccess LUPOOL statement. Care should be taken when coding a generic TCPAccess LU name. If the generic representation matches an LU that is not a TCPAccess Telnet session LU, unnecessary calls will be made to the TCPAccess Telnet server RTM.
2. When you define the Telnet LUs to VTAM, the ACBNAME and NETWORK NAME may differ. Use only the NETWORK NAME on this NetSpy initialization statement.

<b>ACCESS= Values</b>	<b>Explanation</b>
YES	The LU name specified represents a LU defined to a TCPAccess Telnet server.
NO	The LU name specified represents a LU defined to an IBM Telnet server.
<b>Default:</b>	ACCESS=NO

### Notes:

1. Use the ACCESS parameter for TCPAccess Telnet server LUs only.
2. If you coded an ACCSSRTM statement, you must code at least one TELNETLU statement where ACCESS=YES.

<b>FORCEDR= Values</b>	<b>Explanation</b>
ALL	Based on the LU name provided, NetSpy forces a definite response without identifying the Telnet session protocol.
NO	NetSpy only attempts to identify the Telnet session protocol.
TN3270	NetSpy forces a definite response for Telnet sessions identified as TN3270. This value is valid for TCPaccess Telnet sessions and IBM Telnet sessions.
TN3270E	NetSpy forces a definite response for Telnet sessions identified as TN3270E. This value is valid for TCPaccess Telnet sessions and IBM Telnet sessions.
TN3270ER	NetSpy forces a definite response for Telnet sessions identified as TN3270 with the response function negotiated. This value is valid for TCPaccess Telnet sessions only.
<b>Default:</b>	FORCEDR=NO

**Notes:**

1. Use the FORCEDR parameter to make NetSpy force a definite response for sessions in which the application has been identified by an APPL initialization statement coded with the parameters TNMON=YES and FORCEDR=*percentage*.
2. The FORCEDR initialization statement must also be coded.
3. For IBM Telnet sessions, it is not necessary to code a TELNETLU statement with FDR=NO or an APPL statement with TNMON=YES to identify the protocol. However, since the protocol is obtained from the MIB, a SNMPHOST statement must be coded with TCP data collection set to YES.
4. For TCPaccess Telnet server sessions, the protocol is obtained from the TCPaccess Telnet server RTM. The protocol is obtained only when the session's associated application has been defined with the initialization parameter TNMON=YES. The ACCSSRTM statement must also be coded.
5. For NetSpy to force a definite response, both the Access and IBM Telnet sessions must have the associated application defined with the initialization parameter TNMON=YES.
6. Telnet sessions that match the terminal name prefix coded on a FINCLUDE statement are included; Telnet sessions that match the terminal name prefix coded on a FEXCLUDE statement will be excluded.

## TINCLUDE and TEXCLUDE

This statement is optional and tells NetSpy which terminal name prefixes to include (TINCLUDE) or exclude (TEXCLUDE) from monitoring. When you exclude terminals from monitoring, data from these terminals does *not* contribute to the application statistics.

TINCLUDE=*terminal name prefix*  
 TEXCLUDE=*terminal name prefix*

<b>TINCLUDE Prefix Values</b>	<b>Explanation</b>
<i>term prefix 1, term prefix 2, term prefix 3, . . .</i>	The prefixes of terminal names to be included in monitoring, up to the value set in the MAXTCMD statement. Only terminals having names that start with prefixes matching those in TINCLUDE are monitored.
<b>TEXCLUDE Prefix Values</b>	<b>Explanation</b>
<i>term prefix 1, term prefix 2, term prefix 3, . . .</i>	The prefixes of terminal names to be excluded from monitoring, up to the value set in the MAXTCMD statement. Only terminals having names that start with prefixes matching those in TEXCLUDE are not monitored.
Default for TINCLUDE and TEXCLUDE:	If you do not specify TINCLUDE or TEXCLUDE, NetSpy does not treat any terminals specially. All terminals are considered for monitoring.

### Notes:

1. Use only *one* type of statement, either TINCLUDE or TEXCLUDE, but not both. TINCLUDE/TEXCLUDE statements cannot be continued on subsequent lines. You can, however, repeat either statement as often as required.
2. If more than the default number of prefixes (100) are listed in TINCLUDE or TEXCLUDE statements, you *must* specify the MAXTCMD statement before the TINCLUDE or TEXCLUDE statements in the INITPRM file. (See [MAXTCMD](#) in this chapter).
3. NetSpy does not collect response times for printers because they do not send any messages. However, you can exclude them from monitoring with TEXCLUDE. Doing this has no effect on the collection of NCP data.

You can dynamically alter TINCLUDE/TEXCLUDE tables with the SMNR/PMNR commands accessible through NetSpy's operator menu.

## TRACE

This statement tells NetSpy which tracing mode to use.

TRACE=*tracing mode*

Tracing Mode Values	Explanation
INTENSIVE	All transactions that exceed the tracing thresholds are traced. If you use the INTENSIVE parameter, the value for MAXTRACE should be reviewed to ensure that enough buffers are allocated to capture all target transactions.
NORMAL	Transactions are candidates for tracing only after the previous transaction exceeds the tracing threshold.
<b>Default:</b>	TRACE=NORMAL

## TRACEALL

This statement tells NetSpy to activate buffer tracing for the specified terminal. Trace records are written to disk *only* when the trace buffer is full or all TRACEALL requests have been terminated. This means that when a session with a moderate amount of activity is being traced, the trace must be stopped before the records can be printed or displayed.

**Note:** TRACEALL records do not contain response times.

TRACEALL=*luname* [TRLENGTH=*number*] [TRSTARTT=*time*] [TRSTOPT=*time*]

TRACEALL Luname Values	Explanation
<i>VTAM name</i>	The VTAM name of the terminal for which buffer tracing is to be activated.
<b>Default:</b>	If you do not specify TRACEALL, NetSpy will not activate buffer tracing. You can, however, activate tracing online from the Trace Facilities Operator Commands screen.

TRLENGTH Number Values	Explanation
<i>data bytes</i>	The number of data bytes to be traced for each PIU. It affects the traffic for the particular terminal specified on this TRACEALL statement only.
<b>Default:</b>	TRLENGTH=10 (taken from the TRACELLEN parameter)

**TRSTARTT Time Values***hh:mm:ss (or) hh:mm***Default:****Explanation**

The time when the buffer trace specified on this TRACEALL statement is to be activated.

TRSTARTT=00:00

**TRSTOPT Time Values***hh:mm:ss (or) hh:mm***Default:****Explanation**

The time when the buffer trace specified on this TRACEALL statement is to be deactivated.

If this parameter is not specified, the buffer trace will not be stopped.

The following example requests that buffer tracing be activated for the terminal DXAL053. Note that the TRACEALL statement must fit on one line.

```
TRACEALL=DXAL053 TRSTARTT=08:00 TRSTOPT=10:00 TRLENGTH=200
```

## TRACEEXC

This statement tells NetSpy the list of terminal name prefixes for which you want transaction tracing to be disallowed.

TRACEEXC=*terminal name prefix*

**Terminal Name Prefix Values***term prefix 1, term prefix 2, term prefix 3, ...***Default:****Explanation**

The list of terminal prefixes excluded from tracing. Tracing will not be active for terminals listed here.

If you do not specify TRACEEXC, NetSpy will not treat any terminals specially. All terminals will be considered for exception tracing.

**Note:** The TRACEINC and TRACEEXC statements are mutually exclusive. For additional information on defining terminal prefixes, refer to [Terminal Prefix and Generic Name](#) in this chapter.

## TRACEHST

This statement tells NetSpy that if the specified target for host response time is exceeded for a transaction, NetSpy is to trace that transaction.

TRACEHST=*threshold*

Threshold Values	Explanation
<i>time</i>	The target for host response time in tenths of a second. You may specify this parameter either globally or at an individual application level, on an APPL statement.
<b>Default:</b>	If you do not specify TRACEHST, NetSpy will not use host response time on a global level to identify transactions to be traced.

**Note:** You must specify at least one of the three response time thresholds (host, network, or user) for exception tracing to be activated.

## TRACEINC

This statement tells NetSpy the list of terminal name prefixes for which you want exception tracing to be allowed.

TRACEINC=*terminal name prefix*

Terminal Name Prefix Values	Explanation
<i>term prefix 1, term prefix 2, term prefix 3, . . .</i>	The list of terminal name prefixes included in tracing. Tracing will be active only for terminals on this list.
<b>Default:</b>	If you do not specify TRACEINC, NetSpy will not treat any terminals specially. All terminals will be considered for exception tracing.

**Note:** The TRACEINC and TRACEEXC statements are mutually exclusive. For additional information on defining terminal prefixes, refer to [Terminal Prefix and Generic Name](#) in this chapter.

## TRACELEN

This statement tells NetSpy the number of data bytes to trace on an exception basis for each PIU. TRACELEN serves as the default for buffer trace requests, although it can be overridden in that case.

TRACELEN=*length*

<b>Length Values</b>	<b>Explanation</b>
<i>bytes</i>	Number of bytes. The maximum number is 256 bytes.
<b>Minimum:</b>	TRACELEN=0
<b>Maximum:</b>	TRACELEN=256
<b>Default:</b>	TRACELEN=10

**Note:** See the appendix “[System Requirements](#)” for the common storage implications before increasing TRACELEN.

## TRACENET

This statement tells NetSpy that if the specified target for network response time is exceeded for a transaction, NetSpy is to trace that transaction.

TRACENET=*threshold*

<b>Threshold Values</b>	<b>Explanation</b>
<i>time</i>	The threshold for network response time in tenths of a second. You can specify this parameter either globally or at an individual application level (on an APPL statement).
<b>Default:</b>	If you do not specify TRACENET, NetSpy will not use network response time on a global basis to identify transactions to be traced.

**Note:** You must specify at least one of the three response time thresholds (host, network, or user) for exception tracing to be activated.

## TRACEUSR

This statement tells NetSpy that if the specified target for user response time is exceeded for a transaction, NetSpy is to trace that transaction.

TRACEUSR=*threshold*

Threshold Values	Explanation
------------------	-------------

<i>time</i>	The target for user response time in tenths of a second. You may specify this parameter either globally or at an individual application level (on an APPL statement).
-------------	---

<b>Default:</b>	If you do not specify TRACEUSR, NetSpy will not use user response time on a global basis to identify transactions to be traced.
-----------------	---

**Note:** You must specify at least one of the three response time thresholds (host, network, or user) for exception tracing to be activated.

## TRANSGRP

This statement defines a transaction group for a given application. This statement must immediately follow the application's APPL statement.

TRANSGRP=*transaction group name* [TARGET=*targets*]

TRANSGRP Transaction Group Name Values	Explanation
--	-------------

<i>transaction group name</i>	The name of the CA-TPX session identifier (SESSID) used as an alias for the application.
-------------------------------	--

TARGET Target Values	Explanation
----------------------	-------------

<i>target1, target2, target3, target4</i>	Up to four response time distribution targets for the transaction group.
---	--

**Note:** If you want response time distribution statistics for the transaction group to be collected, you must specify at least one target.

## TRCBUFNO

This statement tells NetSpy the number of buffers to dedicate to buffer tracing.

TRCBUFNO=*number*

<b>Number Values</b>	<b>Explanation</b>
<i>buffers</i>	The number of buffers to be dedicated to buffer tracing. The buffer size will be the same as the blocking size for your trace data set. Trace buffers are allocated from CSA only when a TRACEALL request is in effect.
<b>Minimum:</b>	TRCBUFNO=2
<b>Maximum:</b>	Limited by the size of the CSA.
<b>Default:</b>	TRCBUFNO=2

**Note:** If you specify the TRCBUFNO statement with too small a number, PIUs might be missed because there will not be enough buffers to handle the number of concurrent transactions.

## TRCSTART

This statement tells NetSpy when to start tracing specific transactions. It applies to the transaction trace facility only (transaction-all and exception traces). You can specify a starting time for each buffer trace request entered at initialization time with the TRSTARTT parameter on the TRACEALL statement.

TRCSTART=*time*

<b>Time Values</b>	<b>Explanation</b>
<i>hh:mm</i> (or) <i>hh:mm:ss</i>	The hour, minute, and second at which exception tracing is to start.
<b>Default:</b>	If you do not specify TRCSTART, exception tracing and trace alerts will not be activated.

**Note:** If you specify TRCSTART=00:00:00 and TRCSTOP=24:00:00, tracing will never stop.

## TRCSTOP

This statement tells NetSpy when to stop tracing specific transactions. It applies to the exception trace facility only. You can specify a stop time for each buffer trace request entered at initialization time with the TRSTOPT parameter on the TRACEALL statement.

TRCSTOP= *time*

<b>Time Values</b>	<b>Explanation</b>
<i>hh:mm</i> (or) <i>hh:mm:ss</i>	The hour, minute, and second at which exception tracing is to stop.
<b>Default:</b>	TRCSTOP=24:00:00

## USRIDUPD

This statement specifies the interval (in minutes) at which NetSpy searches for all TSO and virtual machine user IDs related to a terminal name, and then updates the sessions with those IDs. Note that user IDs are not displayed for virtual sessions.

USRIDUPD= *interval length*

<b>interval length Values</b>	<b>Explanation</b>
<i>nn</i>	The interval in minutes. Recommended values include one-half or one-third of the interval length specified on the INTERVAL parameter. If you specify USRIDUPD with a time larger than the time specified on INTERVAL, you might not see some of the user IDs.
<b>Default:</b>	If you do not specify USRIDUPD, NetSpy will not search for user IDs.

**Note:** You can view user IDs online from the Terminal Response Time and Traffic screen by pressing the PA2 key.

## UTARGETS

This statement defines the four global user service level objectives (buckets). The UTARGETS statement can be used with the application targets as follows:

- If TARGETS = HOST (application targets) and UTARGETS = `____` then you will have four buckets collecting host response times (on an application basis) and four buckets collecting user response times (on a global basis).
- If TARGETS = USER (application targets) and UTARGETS = `____` then you will have eight buckets collecting user response times (four on a global basis and four on an application basis).

UTARGETS=*objective*

### Objective Values      Explanation

*t1,t2,t3,t4*

These values, specified in tenths of a second, define response time ranges within which NetSpy will count transactions. If you also specified TARGETS=USER, the values you specify for this parameter must be smaller than any of the target values specified in the APPL statement. The reason is because the global values are checked before the values specified on the APPL statement.

Because UTARGETS is a system-wide parameter, the ranges specified in it take effect for all sessions in this host.

### Default:

If you do not specify UTARGETS objectives, NetSpy will not collect global user target data.

### Notes:

1. You can specify either the NTARGETS or the UTARGETS parameter, but you cannot specify both.
2. TARGET must be specified on the APPL statement for the application to record targets.
3. The global buckets are written in the SMF and log records only as Type T and U subtype records.

## VTAMINTF

This statement defines whether the VTAM interface is started when NetSpy is initialized. The VTAM interface allows NetSpy to collect VTAM statistics (application, session, virtual route, and buffer). Use this parameter if you want to split the collection of statistics for storage constraint reasons, or as a way to separate NCP and VTAM information.

VTAMINTF=*option*

<b>Option Values</b>	<b>Explanation</b>
YES	Activates the VTAM interface (as well as the NCP interface) when NetSpy starts. Only one NetSpy can have VTAMINTF=YES specified per host.
NO	The VTAM interface is not activated when NetSpy starts. All statistics except VTAM statistics can be collected. Multiple NetSpys with VTAMINTF=NO specified can run on a single host.
<b>Default:</b>	VTAMINTF=YES

## INITPRM Parameter Quick-Reference

Minimum, maximum, and default parameter values for INITPRM statements are listed in the table below.

Parameter	Minimum	Maximum	Default
ACCSSRTM			None
ACCTING			NO
ALDESC	1	16	None
ALMAXE	11	None	50
ALROUT	1	16	8
ALTBITVL	10	None	30
ALWRITE			INTERVAL
AMAXENT	None	None	100
APPL	1	200	VTAM interface will not be activated
APPLNAME			If APPLNAME=NETNAME is omitted, the ACBNAMEs are assumed.
APLTOAPL			ENHANCED
AUDITCLS			None
BASEITVL	10	None, but must be less than the value of the INTERVAL statement	30
CINCLUDE			(*)
CNFGITVL	30	3600	180
CONSINTF			NO
DBSTART	00:00:00	24:00:00	If not specified, Database logging will not be activated.
DBSTOP	00:00:00	24:00:00	24:00:00 (midnight)
DNSMF			NO
FINCLUDE & FEXCLUDE			All terminals will be considered for FORCEDR if the application specifies it.
FORCEDR			NO

<b>Parameter</b>	<b>Minimum</b>	<b>Maximum</b>	<b>Default</b>
GMAXENT	0	Number of resources in network	100
HCUTOFF			None
HOSTID			OS/390 and z/OS: SMF system ID
HPRDATA			NO
IGNRLOGN			YES
INTERVAL	1	None	15
LANGUAGE			EU
LOGDUMP			NO
LOGSTART	00:00:00	24:00:00	Logging is not started
LOGSTOP	00:00:00	24:00:00	24:00:00 (midnight)
LOGTYPE	0	255	Uses SMF number parameter
LOSTDATA			ONCEONLY
LU62RESP			YES
MAX #NCP	0	Size of region	10
MAX#NRPT	10	300	30
MAXAPPL	None		2 × # applications specified in INITPRM
MAXCA	2	None	30
MAXFCMD	2	Size of CSA*	100
MAXJOBFF	0	100,000	200
MAXLU	2	Size of CSA*	200
MAXNCPSZ	10	Size of region	1000
MAXNOSA	0	9999	5
MAXNOVR	1	239,976	10
MAXOPER	1	Size of region	10
MAXTCMD	2	Size of CSA*	100
MAXTRACE	2	Size of CSA*	Value of MAXLU ÷ by 10
MAXTRALL	2	Size of CSA*	100
MAXTRINC	2	Size of CSA*	100

<b>Parameter</b>	<b>Minimum</b>	<b>Maximum</b>	<b>Default</b>
NCPRETRY	Number: 0 Time: 1	9999	(0,NetSpy-interval)
NCUTOFF			None
NETRSP			DATA
NEUPERF			NEUPERF=OFF
NSYNAME			NETSPY
NSYXNAME			None
NTARGETS			Global network target data will not be collected
NULLTREC			NO
OPTMOD			None
PMI			NO
RIFABNRM			0
RIFNORM			Greater than 0
SECURE			NO
SMF	0, 128	255	0 (no SMF data written).
SMFSTART	00:00:00	24:00:00	00:00:00
SMFSTOP	00:00:00	24:00:00	24:00:00
SMGRID		7 characters	NETSPY@
SNAMDATA			LOCAL
SNMPAGNT			NO
SNMPHOST			None
STOP			STOP=P
SYNC			0
TARGETS			USER
TCPIPMON			NO
TELNETLU			None
TINCLUDE & TEXCLUDE			All terminals considered for monitoring.
TRACE			NORMAL
TRACEALL			Buffer tracing will be inactive

Parameter	Minimum	Maximum	Default
TRACEEXC			All terminals considered for exception tracing
TRACEHST			NetSpy will not use network response time on a global basis to identify transactions to be traced.
TRACEINC			All terminals considered for exception tracing
TRACELEN	0	256	10
TRACENET			NetSpy will not use network response time on a global basis to identify transactions to be traced.
TRACEUSR			NetSpy will not use user response time on a global basis to identify transactions to be traced.
TRANSGRP			None
TRCBUFNO	2	Size of CSA*	2
TRCSTART	00:00:00	24:00:00	Exception and alert tracing will be inactive
TRCSTOP	00:00:00	24:00:00	24:00:00
USRIDUPD			User Ids will not be searched
UTARGETS			Global user target data will not be collected.
VTAMINTF			YES

\* For VTAM Version 3 under OS/390 and z/OS, or MVS/ESA, all CSA is used above 16 MB in virtual storage.

# Defining Startup Parameters

---

## NetSpy Startup Parameters

The control statements in the STARTPRM member or file pertain to the NCPs that NetSpy will monitor, network session and gateway accounting, and NetSpy-to-NetSpy communication. You tailor these parameters to your site's requirements. These statements allow you to define the network by specifying:

- The names of all NCPs, local clusters, local SNA major nodes, and switched nodes, regardless of whether you want to collect performance statistics from them
- The NCP resources for which you want to log statistics

**Note:** NetSpy uses line speed information from an NCP definition to refine its network response time calculations. Consequently, it is important that all NCPs be defined to all NetSpys in your complex. However, since only one NetSpy can establish a session with an NCP to collect its data, you must specify MON=NO in the DEFINE statements for an NCP for all but the one copy of NetSpy that is to collect the NCP data. Typically, you would choose one copy of NetSpy to collect data for all NCPs in your network (MON=YES), and specify MON=NO for all NCPs for all other copies of NetSpy.

To get the full benefit from online reporting, you must define all your NCPs.

### Online Tailoring

You can also define parameters online, as described in the *NetSpy User Guide*.

**WARNING:** *The RRT load module in the NCP load library must be the same one that VTAM used the last time the NCP was activated or errors will occur when NetSpy attempts to collect NPA data.*

## File Names and Formats

When you execute NetSpy on an OS/390 and z/OS system, a set of startup parameters is read from the STARTPRM member of the *dsnpref.NYvvv.CNTL* partitioned data set.

## Notation Conventions

The notation used for representing parameter syntax and information on specifying generic names and terminal prefixes are described in the chapter “Defining Initialization Parameters” in this manual.

## COLLECT Statement

## Purpose

During NetSpy-to-NetSpy communication, this statement enables one or more NetSpys to collect VTAM and NCP data from other NetSpys into its own logging destinations.

## Format

```
COLLECT resource_type [SCOPE=resource] NETSPY=netspyacbx]* [ITVL=mm]
        [LOG=destination] [STARTT=hh:mm] [STOPT=hh:mm]
```

## Operands

Operands for COLLECT are explained below.

Resource_Type	Explanation
<b>Values:</b>	
APPL=name	Generic or specific name of the application
LU=name	Generic or specific name of the LU
NODE=name	Generic or specific name of the node
VR=name	Generic or specific name of the virtual route
<i>Resource_type</i> =*	All known resources of the specified type (APPL, LU, NODE, or VR)

SCOPE=Values	Explanation
<b>Note: The SCOPE values are valid with NODE only.</b>	
LINES	Lines other than X25, NTRI, Ethernet, Frame Relay, and TIC3 lines (for example, ESCON, CLA, SDLC, BSC, and CA)
PUS	Control units other than X25, NTRI, Ethernet, Frame Relay, and TIC3 PUs (for example, ESCON, CLA, SDLC, BSC, and CA)
LUS	LUs other than X25, NTRI, Ethernet, Frame Relay, and TIC3 LUs (for example, ESCON, CLA, SDLC, BSC, and CA)

<b>SCOPE=Values</b>	<b>Explanation</b>
	<b>Note:</b> <i>The SCOPE values are valid with NODE only.</i>
NCPS	NCPs
ONLY	The resource that matches the node name. If you also specify NODE=*, you will get information on all NCPs.
ALL	The node and all resources under it
ALLLINES	All lines
ALLPUS	All PUs
ALLLUS	All LUs
X25LINES	X.25 NCP node monitoring status for all X.25 multi-channel (MCH) lines
X25PUS	X.25 NCP node monitoring status for all X.25 MCH PUs
X25LUS	X.25 NCP node monitoring status for all X.25 LUs
X25VCS	X.25 NCP node monitoring status for all X.25 virtual circuits (VCs)
X25STATS	X.25 NCP node monitoring status for all X.25 MCH lines, MCH PUs, and VCs
X25ALL	X.25 NCP node monitoring status for all X.25 resources
NTRIS	All token ring resources (both physical and logical links)
LLINKS	Logical links on a token ring (TIC)
PLINKS	Physical links on a token ring (TIC)
ETHPLINK	Ethernet physical links
ETHALL	All Ethernet resources
FRPLINK	Frame Relay physical links
FRLINK	Frame Relay logical links
FRPU	Frame Relay physical unit resources, which include LMI stations and FRSE under the physical link
FRALL	All Frame Relay resources
TIC3LINK	TIC3 physical lines
TIC3PU	TIC3 logical PUs
TIC3ALL	Both TIC3 physical lines and logical PUs
<b>Default:</b>	SCOPE=LINES

<b>NETSPY= Values:</b>	<b>Explanation</b>
<i>netspyachx</i>	The specific name on the NSYXNAME parameter in the INITPRM member of the remote NetSpy
*	All known remote NetSpys

<b>ITVL= Values:</b>	<b>Explanation</b>
<i>mm</i>	A collection interval in minutes. The value must be a multiple of the base interval in the remote NetSpy. If you want the response times to be synchronized between the collection interval on this statement and the interval in the remote NetSpy, specify a collection interval identical to the one used in the remote NetSpy.
<b>Default:</b>	The interval time specified in the remote NetSpy

<b>LOG= Values:</b>	<b>Explanation</b>
LOG	Tells NetSpy to log to the Log only (Default)
SMF	Tells NetSpy to log to SMF <i>and</i> the Log
DB	Tells NetSpy to log to the Database only
(SMF)	Tells NetSpy to log to SMF only
<b>Default:</b>	LOG=LOG

**Note:** Multiple destinations can be enclosed in parentheses and separated by commas. For example, LOG=(LOG,SMF,DB) logs data to all three destinations. If you want to specify SMF as the *only* destination, you must use parentheses, like this: LOG=(SMF).

<b>STARTT= and STOPT= Values:</b>	<b>Explanation</b>
<i>hh:mm:ss (or) hh:mm</i>	Time relative to the local NetSpy when you want data collection to start and stop, respectively. NetSpy converts this time to the remote NetSpy time.
<b>Default:</b>	STARTT: The current time STOPT: None
	<b>Note:</b> If you specify a start time and STOPT=99:99:99, data collection runs continuously.

---

**Note:** The start and stop times place the COLLECT commands in a timer queue on the local NetSpy, where they are issued at the appropriate start and stop times. The only time you would specify a stop time with no start time would be to update an old stop time or supply a stop time that was not previously given. A stop time without a start time does not assume a start time value.

---

## Usage

Note the following about the COLLECT statement:

1. To get the most flexibility, specify a COLLECT statement with a start and stop time for each major resource name (especially for NODE) and NetSpy. NetSpy collects different records for each resource type:
  - For APPLs, type A records
  - For LUs, type T and U records
  - For NODEs, type N records
  - For VRs, type V records
2. If a NetSpy-to-NetSpy session goes down when the local NetSpy is receiving data from a remote NetSpy, the remote NetSpy continues to collect data until the collection interval expires. Then, if the collection stop time has not expired when the session is reestablished, the local NetSpy automatically issues a COLLECT command identical to the initial COLLECT statement. As a result:
  - If the collection interval has not expired at the remote NetSpy, the remote NetSpy ignores the new command and collection continues as if the session had not been broken
  - If the collection interval has expired at the remote NetSpy, collection in the remote NetSpy is restarted
3. In conjunction with this statement, make sure that you also specify the following:
  - The NSYXNAME statement in the INITPRM member or file of each remote NetSpy specified on the COLLECT statement
  - The CONNECT statement in the STARTPRM member or file of the local NetSpy to establish a session between it and the remote NetSpys
4. After startup, you can change how the local NetSpy collects data from remote NetSpys by issuing the COLLECT command online. For more information, see the *NetSpy User Guide*.

## COLLECT POLLSTAT Statement

**Purpose** This statement enables the transfer of polling statistics during NetSpy-to-NetSpy communication. It directs the remote NetSpy identified by *netspyacb*x to collect polling statistics and transfer the data to the requesting NetSpy for the purpose of calculating response time. The remote NetSpy collects the polling data and transfers updated information at every base interval (as specified on the BASEITVL parameter in INITPRM).

NetSpy uses this NCP information to calculate response time when definite response times are not available and for NCP statistics on the Terminal Response Time Analysis screen when a destination NetSpy is specified.

**Format**

```
COLLECT POLLSTAT NODE=nodename NETSPY=netspyacbx
```

**Operands**

Operands for COLLECT POLLSTAT are described below.

<b>NODE= Values:</b>	<b>Explanation</b>
<i>nodename</i>	Indicates that you want NetSpy to collect polling data on the NCP resource that has this name. <i>Nodename</i> can be specified as a generic name.
<b>NETSPY= Values:</b>	<b>Explanation</b>
<i>netspyacb</i> x	The specific name on the NSYXNAME parameter in the INITPRM member of the remote NetSpy
<b>Default:</b>	None

**Usage**

Note the following:

- The NCP source must be defined to both NetSpys that are collecting and receiving poll statistics. The receiving NetSpy does not need to be monitoring.
- You can specify the COLLECT POLLSTAT statement only in the startup parameters (STARTPRM).
- No message is issued at startup time for this command.
- If a COLLECT POLLSTAT statement is being used for an NCP, no SSMF statements should be used for that NCP.

## CONNECT Statement

**Purpose** This statement tells NetSpy to establish a NetSpy-to-NetSpy session between this NetSpy and a remote NetSpy. The name on this statement must match the name specified on the NSYXNAME parameter in INITPRM for the other NetSpy.

**Note:** You *must* specify the NSYXNAME parameter in INITPRM to enable the CONNECT parameter in STARTPRM.

**Format**

CONNECT *netspyacb*

**Operands**

Operands for CONNECT are explained below.

Operand	Explanation
<i>netspyacb</i>	The VTAM ACB name specified on the NSYXNAME parameter of the NetSpy you want to be in session with your copy of NetSpy
<b>Default:</b>	This parameter has no default. If you omit it, NetSpy will not initiate any sessions with other NetSpys at startup.

**Usage**

For NetSpy-to-NetSpy communication, only one side of the NetSpy-to-NetSpy communication needs to code this statement. You should code this statement in the initialization parameters of the NetSpy into which you want to collect or receive remote NetSpy data. The NetSpy with this statement coded becomes a SLU. The NetSpy associated with the ACB name, “*netspyacb*” coded in this statement becomes the PLU.

**Note:** For NetMaster-to-NetSpy communication, NetSpy can only be a PLU. In other words, do not code this statement using an acbname associated with a NetMaster address space. NetSpy cannot initiate a connection with a NetMaster ACB. However, NetMaster can request a session with a NetSpy using the ACB name, *netspyacb* coded on the NSYXNAME parameter. See the NetMaster documentation for the required parameters.

**Example**

Here is an example of a CONNECT statement:

```
CONNECT NETSPY=NETSPYZZ
```

You would specify this statement in NETSPYXX, informing this NetSpy to communicate with NETSPYZZ. NETSPYZZ would not need a statement telling it to communicate with NETSPYXX. The statement needs to appear in *only one* of the STARTPRM members.

## How to Start NetSpy-to-NetSpy Communication

To establish a session between two or more NetSpys, take the following actions:

1. Specify `NSYXNAME=name` in `INITPRM`.  
 This causes the associated ACB name to be OPENED and the VTAM environment to be established. Before a NetSpy or NetMaster can successfully connect to a NetSpy, both sides of the communication must have an ACTIVE/ OPENED ACB and an established VTAM environment.
2. Specify the appropriate APPL statements in your VTAM definitions.  
**Note:** The JCLAPPL member of the `dsnpref.NYvvv.CNTL` file contains examples of the definitions you need.
3. Specify `CONNECT NETSPY=name` in `STARTPRM`, or issue the command, `CONNECT name`, from the command line of any NetSpy screen. For more information, see the *NetSpy User Guide*.

**Note:** Do not connect NetSpys that are not at the same release. The results are unpredictable.

## DEFINE Statement

**Purpose** This statement requests NetSpy to search the NCP source library for *name* in order to define the corresponding NCP.

This file is identified by the `//NCPSRC DD` statement in your NetSpy procedure.

**Format**

```
DEFINE ncpname|ncp*|majnode MON=YES|NO NPALU=npaluname
      [RETRY=number|(number, time)] NTYPE=NWAYS
```

**Operands** Operands for DEFINE are explained below.

DEFINE Values:	Explanation
<i>ncpname</i>	Indicates the NCP to be defined to NetSpy. NetSpy reads the NCP source code to determine all of the resources associated with this NCP. You should define the <i>ncpname</i> before making other references to any resource in this NCP.
<i>ncp*</i>	Indicates an NCP, specified as a generic name, to be defined to NetSpy. Using a generic name prevents you from having to redefine an NCP to NetSpy if you regenerate the NCP. Specify the first character(s) of the NCP name then an asterisk. The asterisk can represent up to six alphanumeric

characters (to a maximum of seven in the NCP name). All possible NCP names represented by the generic name should have the same subarea, which should be unique across all DEFINE statements.

If a specific NCP definition and a generic NCP definition overlap, the first occurrence is used.

**Note:** Generic names are supported in the OS/390 and z/OS environment only.

*majnode* Indicates a non-NCP major node name to be defined to NetSpy. NetSpy reads the major node source to determine all the resources associated with this major node. Major node types are local clusters, local SNA major nodes, and switched nodes.

**Default:** None

**MON= Values: Explanation**

YES Indicates that NetSpy is to establish a session with the NPA pseudo-LU defined in the NCP generation.

If using a generic NCP name, NetSpy defines only one NCP, either:

- The NCP that successfully acquires the NPALU, or
- The NCP whose RRT has the latest date/time stamp. NetSpy continues trying to acquire this NCP NPALU session based on the values specified on the RETRY operand.

Later, if an NCP with the same subarea becomes active and VTAM tries to LOGAPPL the NPALU to NetSpy, and NetSpy's definition for the NCP with that subarea is not the one loaded, all possible matches are reprocessed to locate the correct NCP. NetSpy automatically deletes the old definition, builds the new one and ACQUIRES the NPALU. All generic SSMF and NETACCT statements for this node are applied to the newly defined NCP.

**Note:** To locate the active NCP, NetSpy attempts to BIND each NCP that matches the generic name and that exists in both the source and load libraries. To decrease startup overhead and to avoid excessive console messages for failed BINDs, the number of NCPs that match the generic name should be kept to a minimum.

<b>MON= Values:</b>	<b>Explanation</b>
NO	Indicates that NetSpy is not to establish this session. If using a generic NCP name, NetSpy defines either: <ul style="list-style-type: none"> <li>▪ The NCP whose RRT has the latest date/time stamp, or</li> <li>▪ The first NCP found in the NCP source library that matches the generic specification</li> </ul>
<b>Default:</b>	MON=YES (for NCPs only); MON=NO (for non-NCPs)

<b>NPALU= Values:</b>	<b>Explanation</b>
<i>npalu name</i>	Specifies the NCP NPALU node with which you want NetSpy to be in session. You can start multiple NetSpy sessions with the same NCP provided that: Each session involves a different NPALU. The last NetSpy session started is the one that acquires the first NPALU defined in the NCP.
<b>Default:</b>	The first NPALU defined in the NCP.

<b>RETRY= Values:</b>	<b>Explanation</b>
<i>number</i>	Indicates the number of times NetSpy will try to acquire an NCP's NPALU session after the session has been lost or an attempt to acquire it has failed. Valid values are 0 to 9999.
<i>time</i>	Indicates the time between retries in minutes. Valid values are 1 to 9999.
<b>Default:</b>	NCPRETRY=(0,NetSpy-interval)

<b>NTYPE= Values:</b>	<b>Explanation</b>
NWAYS	Indicates you are using an IBM 3746 Nways Multiprotocol controller Model 950 (which does not require an NCP). If you code this parameter, you must also specify NPALU= <i>npaluname</i> .  <b>Note:</b> All NetSpy statements and commands that are valid for NCPs are valid for N Ways controllers as well.

For more information on the DEFINE command, see Using the Operator Command Menu in the chapter "Displaying Real-time Data" in the *NetSpy User Guide*.

## NETACCT Statement

**Purpose** This statement tells NetSpy to begin collecting network accounting statistics and where to write them. It also tells the NCP to send accounting statistics to NetSpy when the specified byte (BTH) and PIU (PTH) thresholds have been reached. If you want to collect both session and gateway accounting, you must specify two different NETACCT statements.

**Format**

```
NETACCT=option [ALOG=option] [NCP=option] [BTH=threshold]
                [PTH=threshold] [PIUDIST=n1:n2:n3:n4:n5:n6]
```

**Operands** Operands for NETACCT are explained below.

---

### NETACCT=Values: Explanation

---

NSA	Turns on network session accounting.
GWA	Turns on network gateway accounting.
NO	Neither network session nor gateway accounting is being used.
<b>Default:</b>	NETACCT=NO

---

### ALOG= Values: Explanation

---

LOG	Logs the network accounting records to the Log.
SMF	Logs the network accounting records to SMF.
DB	Logs the network accounting records to the Database.
<b>Default:</b>	ALOG=LOG

---

**Note:** Multiple destinations are not supported for the network accounting records.

---

<b>NCP= Values:</b>	<b>Explanation</b>
<b>Note:</b> This parameter is required for gateway and session accounting.	
<i>ncpname</i>	Indicates that NetSpy should begin collecting accounting statistics from this particular NCP.  You can specify the <i>ncpname</i> as a generic name by placing an asterisk (*) at the end of the name. The asterisk represents up to six alphanumeric characters and must match the generic <i>ncpname</i> on a previous NCP DEFINE statement.
ALL or *	Indicates that NetSpy should begin collecting accounting statistics for all NCPs listed in the DEFINE statements.
<b>Default:</b>	None
<b>Notes:</b>	
<ul style="list-style-type: none"> <li>▪ For network session accounting, all NCPs you name in the NETACCT statement must have been previously defined in the DEFINE statements in the NCP startup parameters. You can specify more than one NETACCT statement for different NCPs.</li> <li>▪ Gateway accounting can be collected only from the NCPs that are defined as gateway NCPs with the gateway accounting statement specified in the NCP gen. For more information on gateway accounting, see the <i>NetSpy User Guide</i>.</li> <li>▪ NCPs do not have to collect performance statistics (SSMF) in order to collect accounting records.</li> </ul>	
<b>BTH Threshold Values:</b>	<b>Explanation</b>
<i>number</i>	Sets the byte threshold in the NCP to specify when network accounting statistics should be sent over the NPALU to NetSpy.
<b>Default:</b>	BTH value on the SESSACC/GWSESAC parameter on the BUILD statement. If you did not specify a byte threshold on the SESSACC/GWSESAC parameter, NetSpy uses a default of BTH=25000.

<b>PTH Threshold Values:</b>	<b>Explanation</b>
<i>number</i>	Sets the PIU threshold in the NCP to specify when network accounting statistics should be sent over the NPALU to NetSpy.
<b>Default:</b>	PTH value on the SESSACC/GWSESAC parameter on the BUILD statement. If you did not specify a PIU threshold on the SESSACC/GWSESAC parameter, NetSpy uses a default of PTH=2500.
<b>PIUDIST Target Values:</b>	<b>Explanation</b>
<i>n1:n2:n3:n4:n5:n6</i>	Sets six PIU distribution ranges for the sessions monitored for network accounting: <i>n1</i> through <i>n6</i> must be in ascending order. (The NCP must have been generated with a value of zero or higher in the SESSACC or GWSESAC parameter.)
<b>Default:</b>	PIUDIST=0 (No PIU distribution list is defined initially. If desired, you can change the ranges online. The NCP must have been generated with a value of zero or more in the SESSACC or GWSESAC parameter.)

## Usage

To use network session accounting, you must generate the NCP by specifying NPA=YES and SESSACC=YES. NetSpy will use the NCP SESSACC parameters specified for the PIU and byte thresholds. If no values are specified for these thresholds, NetSpy uses the following defaults:

For NCP V5.4 or above: SESSACC=(YES,ALL,,25000,2500)  
 For NCP V4.3.1: SESSACC=(YES,ALL,,25000,2500,,(0))

In the default statements above:

- ALL**        Requests accounting on both PLU and SLU sessions.
- 25000**      The byte threshold.
- 2500**        The PIU threshold.
- 0**            No PIU distribution list is defined initially. (You can define one online.)

**Note:** To use network gateway accounting (with NCP V4.3.1), you must generate the NCP as a gateway NCP with the NPA=YES, SESSACC, and GWSESAC statements. If no values are specified for these thresholds, NetSpy uses the following defaults:

SESSACC=(YES,ALL,,25000,2500,,(0))  
 GWSESAC=(YES,,,25000,2500,,(0))

## SSMF Statement

**Purpose** This statement requests NetSpy to start collecting NCP data and logging it for a node within a previously defined NCP.

**Format** SSMF [*nodename*] [SCOPE=*resource*] [START=*hh:mm*] [STOPT=*hh:mm*]

**Operands** Operands for SSMF are explained below.

SSMF= Values:	Explanation
<i>nodename</i>	The particular node (NCP, line, controller, or terminal) for which NetSpy is to collect NCP data and log it.  You can specify the <i>nodename</i> as a generic name by placing an asterisk (*) at the end of the name. The asterisk represents up to six alphanumeric characters and <b>must match</b> the generic <i>ncpname</i> on a previous NCP DEFINE statement.
<b>Default:</b>	None.

SCOPE= Values:	Explanation
LINES	The node, all non-NTRI, and non-X.25 lines within
PUS	The node, all non-NTRI, and all non-X.25 controllers within
LUS	The node, all non-NTRI, and all non-X.25 terminals within
ONLY	This node only
ALL	All resources
X25LINES	All X.25 multi-channel (MCH) lines for the specified node
X25PUS	The node (if it is an X.25 MCH line resource) all X.25 MCH physical units for the specified node
X25VCS	All X.25 virtual circuits for the specified node
X25STATS	All X.25 virtual circuits, X.25 MCH lines, and X.25 MCH physical units for the specified node
X25LUS	The node (if it is an X.25 virtual circuit) and all X.25 logical units for the specified node
X25ALL	All X.25 resources for the specified node
NTRIS	All token ring (TIC) resources (both physical and logical links)

<b>SCOPE= Values:</b>	<b>Explanation</b>
LLINKS	All logical links on a token ring (TIC)
PLINKS	All physical links on a token ring (TIC)
ALLLINES	The node and all lines within
ALLPUS	The node and all control units within
ALLLUS	The node and all terminals within
FRPLINK	Frame Relay physical link resources
FRLINK	Frame Relay logical link resources
FRPU	Frame Relay physical unit resources
FRALL	All Frame Relay resources
ETHPLINK	Ethernet physical link resources
ETHALL	All Ethernet resources
TIC3LINK	TIC3 physical line resources
TIC3PU	TIC3 logical PU resources
TIC3ALL	Both TIC3 physical lines and logical PUs
<b>Default:</b>	SCOPE=ONLY

**Note:** NetSpy does not implicitly collect data for lines that connect physical logical units. To collect data for lines *and* their connected units, you can specify multiple SSMF statements with the same node name and different scopes. For example:

```
SSMF node2 SCOPE=LINES
SSMF node2 SCOPE=PUS
```

When you dynamically add a device that falls within the scope of an existing SSMF statement, NCP data collection and logging occurs automatically for that device. (**Note:** Devices added dynamically are reported to NetSpy only if you specified the NPA=(YES,DR) parameter on the BUILD definition statement.)

<b>START= and STOPT= Values:</b>	<b>Explanation</b>
<i>hh:mm or hh:mm:ss</i>	The time at which data collection is to start or stop
<b>Default:</b>	Data collection starts immediately and continues until the user stops it.



# Defining Monitors for General Alerts

---

## Defining General Alert Monitors

You define monitors for general alerts in two ways, through:

- MONITOR statements in the ALERTPRM member or file
- The Define Monitors option on the NetSpy Main Menu

MONITOR statements tell NetSpy which resources to monitor for alerts and how often, which criteria will generate alerts, and where alert data will be sent. Each time NetSpy starts up, it reads these statements to find out what to monitor and how to generate and handle alerts.

The AMAXENT statement in the INITPRM member or file determines the number of MONITOR statements that you can specify. This limit applies to monitors created through both MONITOR statements and the Define Monitors option on the NetSpy Main Menu. For more information, see the *NetSpy User Guide*.

### ALERTPRM File Names and Formats

Monitor statements are located in the ALERTPRM member of the *dsnpref.NYvvv.CNTL* data set. When you install NetSpy, this member is copied onto your system.

### Monitor Status Display

You can find out which monitors are active through the Monitor Status Display. To see this display, do one of the following:

- On the General Alert System Selection Menu, select option 3, Display Monitor Status.
- On the command line of any NetSpy screen, enter DISMON.

## Monitor Statement Syntax

This chapter uses the following notation when describing the syntax of MONITOR statements.

<b>UPPERCASE</b>	Keywords in all uppercase must be entered exactly as shown.
<i>italics</i>	Italics indicate a variable for which you must supply a value.
[ ]	Brackets indicate the keyword is optional.
{ }	Braces indicate mutually exclusive required operands. You must choose one.  <b>Note:</b> For threshold definitions in MONITOR statements, you may choose more than one.
	A vertical bar means you must choose between mutually exclusive values.

### VTAM vs. NCP Data

Note that the MONITOR statement for VTAM data is slightly different from the statement for NCP data. Both types of statements and their parameters are explained in the following sections.

## For VTAM Data

The format of the MONITOR statement for VTAM data is:

```

MONITOR NAME=monname {APPL=name} {AHRSP>or<n} [EXCLU62|ONLYLU62]
                        {ANRSP>or<n}
                        {AURSP>or<n}
                        {BYTERATE>or<n}
                        {TRANRATE>or<n}
                        {WHRSP>or<n}
                        {WNRSP>or<n}
                        {#SESS>or<n}

                        {LINE=name} {AHRSP>or<n} [EXCLU62|ONLYLU62]
                        {ANRSP>or<n}
                        {AURSP>or<n}
                        {MSGRATE>or<n}
                        {BYTERATE>or<n}
                        {TRANRATE>or<n}
                        {WHRSP>or<n}
                        {WNRSP>or<n}

                        {LU=name} {AHRSP>or<n} [FORAPPL=name]
                        {ANRSP>or<n} [FORLINE=name]
                        {AURSP>or<n} [FORPU=name]
                        {MSGRATE>or<n} [EXCLU62|ONLYLU62]
                        {BYTERATE>or<n}
                        {TRANRATE>or<n}
                        {WHRSP>or<n}
                        {WNRSP>or<n}

                        {PU=name} {AHRSP>or<n} [EXCLU62|ONLYLU62]
                        {ANRSP>or<n}
                        {AURSP>or<n}
                        {MSGRATE>or<n}
                        {BYTERATE>or<n}
                        {TRANRATE>or<n}
                        {WHRSP>or<n}
                        {WNRSP>or<n}

                        {VR=name} {ANRSP>or<n}
                        {BHELD>or<n}
                        {PIURATE>or<n}
                        {OPIURATE>or<n}
                        {IPIURATE>or<n}

[MATCH=option] [ITVL=n] [TITLE='text'] [STARTT=time]
[STOPT=time] [DEST=option] [NSYXNAME=netname]

```

## For NCP Data

The format of the MONITOR statement for NCP data is:

```

MONITOR NAME=monname {LINE=name} [ERRS>or<n]
                                [OQLen>or<n]
                                [PIURATE>or<n]
                                [UTL>or<n]
                                [RBYTES>or<n]
                                [RMSGs>or<n]

                                {NCP=name} [CCU>or<n]
                                           [CHQ>or<n]
                                           [UBUF>or<n]

                                {PU=name} [ERRS>or<n]
                                           [OQLen>or<n]
                                           [PIURATE>or<n]
                                           [UTL>or<n]
                                           [RBYTES>or<n]
                                           [RMSGs>or<n]

                                {X25LINES=name} [UTL>or<n]
                                                [IFRMM>or<n]
                                                [OQLen>or<n]

                                {X25PUS=name} [PACKM>or<n]

                                {X25VCS=name} [PACKM>or<n]

                                {PLINKS=name} [UTL>or<n]
                                                [IFRMM>or<n]
                                                [BYTESS>or<n]
                                                [OQLen>or<n]
                                                [RIFRMS>or<n]
                                                [RBYTES>or<n]
                                                [CONGSCNT>or<n]
                                                [ACTCONS>or<n]

                                {LLINKS=name} [TIMEOUTS>or<n]
                                                [IFRMM>or<n]
                                                [BYTESS>or<n]
                                                [OQLen>or<n]
                                                [RIFRMS>or<n]
                                                [RBYTES>or<n]

                                {ETHPLINK=name} [DFRMS>or<n]
                                                [IFRMM>or<n]
                                                [BYTESS>or<n]
                                                [OQLen>or<n]
                                                [CONGSCNT>or<n]
                                                [TRANSDEF>or<n]
                                                [ONECOLL>or<n]
                                                [MULTCOLL>or<n]

                                {FRPLINK=name} [DFRMS>or<n]
                                                [IFRMM>or<n]
                                                [BYTESS>or<n]
                                                [OQLen>or<n]
                                                [RBYTES>or<n]
                                                [RIFRMS>or<n]
                                                [CONGSFWD>or<n]
                                                [CONGSBCK>or<n]
    
```

---

```
{FRLINK=name} [IFRMM>or<n]  
                [BYTESS>or<n]  
                [OQLN>or<n]  
                [RBYTES>or<n]  
                [RIFRMS>or<n]  
                [CONGSFWD>or<n]  
                [CONGSBCK>or<n]  
  
{FRPU=name} [IFRMM>or<n]  
              [BYTESS>or<n]  
              [OQLN>or<n]  
              [DFRMS>or<n]  
              [CONGSFWD>or<n]  
              [CONGSBCK>or<n]  
  
{TIC3LINK=name} [IFRMM>or<n]  
                 [BYTESS>or<n]  
                 [DFRMS>or<n]  
                 [RIFRMS>or<n]  
                 [RBYTES>or<n]  
                 [EFRMS>or<n]  
                 [UTL>or<n]  
  
{TIC3PU=name} [IFRMM>or<n]  
               [BYTESS>or<n]  
               [RIFRMS>or<n]  
               [RBYTES>or<n]  
               [REJFRMS>or<n]  
               [TIMEOUTS>or<n]  
               [EFRMS>or<n]  
               [UTL>or<n]  
  
[MATCH=option] [ITVL=n] [TITLE='text'] [STARTT=time]  
[STOPT=time] [DEST=option] [NSYXNAME=netname]
```

## Monitor Statement Operands

The following sections describe all the operands for the MONITOR statement.

### Monitor Name

Assign a name to the monitor, up to eight characters in length. For example,

```
MONITOR NAME=MONITOR1
```

### MONITOR Resource Types

On each MONITOR statement, you must specify one of the resource types in the table below.

Valid *names* include:

- Specific name
- Generic name
- An asterisk (\*), representing all resources of that type
- Resource list, containing a list of resources of that type (for example, APPL=(CICS, IMS, NETSPY))
- A list of files containing names of resources of that type (for example, APPL=FILE(MEMBER1, MEMBER2), where MEMBER1 and MEMBER2 are data sets that reside in RSCPARM DD which contain lists of resources).

Resource	Description
APPL	Application and any transaction groups defined for it (on the TRANSGRP statement in INITPRM)
ETHPLINK	Ethernet physical link
FRLINK	Frame Relay logical link
FRPLINK	Frame Relay physical link
FRPU	Frame Relay PU
LINE	Line
LLINKS	NTRI logical link
LU	LU (logical unit)
NCP	NCP (Network Control Program)
PLINKS	NTRI physical link

Resource	Description
PU	PU (physical unit)
TIC3LINK	TIC3 (High Performance Token Ring interface) physical line
TIC3PU	TIC3 logical PU
VR	VR (virtual route)
X25LINES	X25 line
X25PUS	X25 PU
X25VCS	X25 VC (virtual circuit)

## MONITOR Threshold Variables

At least one of the threshold parameters in the table below is required on each MONITOR statement. You can specify up to nine of these parameters in one statement. If you wish to specify a range, use the same variable twice. For example: AURSP<3 AURSP>0.

Variable Type	Description
ACTCONS	Number of active connections during the interval. Valid with PLINKS resources only.
AHRSP	Average host response time during the interval. Valid with APPL, LINE, LU, and PU resources only.
ANRSP	Average network response time during the interval. Valid with APPL, LINE, LU, PU, and VR resources only.
AURSP	Average user response time during the interval. Valid with APPL, LINE, LU, and PU resources only.
BHELD	Percentage of virtual routes blocked or held during the interval. Valid with VR resources only.
BYTERATE	Number of bytes per second that the resource sends or receives during the interval. Valid with APPL, LINE, LU, and PU resources only.
BYTESS	Number of bytes per second that the resource sends or receives during the interval. For TIC3 resources, the number of IFRAMES per second. Valid with PLINKS, LLINKS, ETHPLINK, FRPLINK, FRLINK, FRPU, TIC3LINK, and TIC3PU resources only.
CCU	NCP cycle utilization. Valid with NCP resources only.

<b>Variable Type</b>	<b>Description</b>
CHQ	Channel hold queue (the number of messages sent to the host, but not yet acknowledged). Valid with NCP resources only.
CONGSBCK	Congestion back. Valid with FRPLINK, FRLINK, and FRPU resources only.
CONGSCNT	Congestion count during the interval. Valid with PLINKS and ETHPLINK resources only.
CONGSFWD	Congestion forward. Valid with FRPLINK, FRLINK, and FRPU resources only.
DFRMS	Number of IFRAMES that are discarded during the interval. Valid with FRPLINK, FRPU, TIC3LINK, and ETHPLINK resources only.
EFRMS	Number of error frames. For physical links, this is the sum of misaddressed, discarded, and unrecognized frames. For logical PUs, this is the total of rejected frames sent and received. Valid with TIC3LINK and TIC3PU resources.
ERRS	Number of errors that occur during the interval. Valid with LINE and PU resources only.
IFRMM	Number of IFRAMES per minute. For TIC3 resources, the percentage of TIC being utilized. Valid with X25LINES, PLINKS, LLINKS, ETHPLINK, FRPLINK, FRLINK, FRPU, TIC3LINK, and TIC3PU resources only.
IPIURATE	Number of PIUs per minute that the resource receives. Valid with VR resources only.
MSGRATE	Number of messages per minute that the resource sends or receives. A complete PIU chain constitutes a message. Valid with LINE, LU, and PU resources only.
MULTCOLL	Number of multiple collisions during the interval. Valid with ETHPLINK resources only.
ONECOLL	Number of single collisions during the interval. Valid with ETHPLINK resources only.
OPIURATE	Number of PIUs per minute that the resource sends. Valid with VR resources only.
OQLEN	Outbound queue length (the number of messages queued to be output). Valid with LINE, PU, X25LINES, PLINKS, LLINKS, ETHPLINK, FRPLINK, FRLINK, and FRPU resources only.
PACKM	Number of packets per minute. Valid with X25PUS and X25VCS resources only.

<b>Variable Type</b>	<b>Description</b>
PIURATE	Number of PIUs per minute that the resource sends and receives. Valid with LINE, PU, and VR resources only.
RBYTES	Number of bytes that are retransmitted during the interval. For LINE and PU, the percentage of bytes retransmitted. Valid with LINE, PU, PLINKS, LLINKS, FRPLINK, FRLINK, TIC3LINK, and TIC3PU resources only.
REJFRMS	Number of sent/received frames that were rejected during the interval. Valid with TIC3PU resource only.
RIFRMS	Number of IFRAMEs that are retransmitted during the interval. Valid with PLINKS, LLINKS, FRPLINK, FRLINK, TIC3LINK, and TIC3PU resources only.
RMSGs	Percentage of messages retransmitted during the interval. Valid with LINE and PU.
TIMEOUTS	Number of timeouts (for TIC3PU, the number of LAN T2 timeouts) that occurred during the interval. Valid with LLINKS and TIC3PU resources only.
TRANRATE	Number of transactions per minute that the resource sends or receives. Valid with APPL, LINE, LU, and PU resources only.
TRANSDEF	Number of transmissions deferred during the interval. Valid with ETHPLINK resources only.
UBUF	Percentage of the NCP buffer used during the interval. Valid with NCP resources only.
UTL	Percentage of the resource used during the interval. If primary or secondary utilization thresholds are exceeded, an alert is generated. Valid with LINE, PU, X25LINES, PLINKS, TIC3LINK, and TIC3PU resources only.
WHRSP	Worst host response time during the interval. Valid with APPL, LINE, LU, and PU resources only.
WNRSP	Worst network response time during the interval. Valid with APPL, LINE, LU, and PU resources only.
#SESS	Number of sessions running concurrently with the application during the interval. Valid with APPL resources only.

## MONITOR Optional Operands

You can specify one or more of the parameters in the table below on each MONITOR statement.

Parameter	Description
DEST	<p>Specifies where NetSpy sends alert data. If desired, you can specify multiple destinations enclosed in parentheses and separated by commas, for example: DEST=(CONSOLE,LOG). Valid destinations include:</p> <ul style="list-style-type: none"> <li>■ ALL, for all possible destinations</li> <li>■ CONSOLE, for the system console</li> <li>■ DB, for the Database</li> <li>■ GLOBAL, for the Global Alerts Display, which only privileged NetSpy users can access</li> <li>■ LOG, for the Log</li> <li>■ NETVIEW <b>Note:</b> If you specify NetView as the destination, you view the alerts in NPDA, the NetView alert display facility</li> <li>■ NMEPS, for the NetMaster EPS receiver. This option is mutually exclusive with the NetView option.</li> <li>■ NSYLOG, for the Log (alias of LOG)</li> <li>■ SMF, for SMF</li> <li>■ SNMP, for Unicenter and other SNMP managers. These alerts can be viewed on the Global Alerts Display.</li> </ul> <p>DEST defaults to LOG.</p>
EXCLU62	Excludes LU 6.2 information
FORAPPL	<p>Specifies the applications to be monitored for alerts. Valid names include:</p> <ul style="list-style-type: none"> <li>■ <i>applname</i>, for the application that NetSpy is to monitor</li> <li>■ <i>resource list</i>, for the resource list containing a list of the applications to monitor</li> </ul> <p>For example, you may specify FORAPPL=FILE(<i>applfile</i>) or FORAPPL=(APPL1,APPL2).</p> <p>Valid with LUs only.</p>

Parameter	Description
FORLINE	<p>Specifies the lines to be monitored for alerts. Valid names include:</p> <ul style="list-style-type: none"> <li>■ <i>linename</i>, for the line that NetSpy is to monitor</li> <li>■ <i>resource list</i>, for the resource list containing a list of the lines to monitor</li> </ul> <p>For example, you may specify FORLINE=FILE(<i>linefile</i>) or FORLINE=(LINE1,LINE2).</p> <p>Valid with LUs only.</p>
FORPU	<p>Specifies the clusters to be monitored for alerts. Valid names include:</p> <ul style="list-style-type: none"> <li>■ <i>clustername</i>, for the cluster that NetSpy is to monitor</li> <li>■ <i>resource list</i>, for the resource list containing a list of the clusters to monitor</li> </ul> <p>For example, you may specify FORPU=FILE(<i>pufile</i>) or FORPU=(PU1,PU2).</p> <p>Valid with LUs only.</p>
ITVL	<p>Specifies the interval at which NetSpy checks the resources for alerts. Specify a value of at least 30 seconds (the default).</p>
MATCH	<p>Specifies the conditions that must be met before an alert is generated. Valid options include:</p> <ul style="list-style-type: none"> <li>■ ALL, to generate alerts only if all of the specified thresholds are exceeded</li> <li>■ ANY, to generate alerts if at least one of the specified thresholds is exceeded</li> </ul> <p>MATCH defaults to ALL.</p>
NAME	<p>Up to eight characters that uniquely identify the monitor</p>
NSYXNAME	<p>Specifies one or more cross-domain NetSpys to which you want to send the MONITOR statement for execution.</p> <p>Specify the specific or generic NSYXNAME of the NetSpy on which the monitor is run. Specifying an asterisk (*) indicates all NetSpys.</p> <p>NSYXNAME defaults to the local NetSpy that contains this ALERTPRM member or file.</p>
ONLYLU62	<p>Includes only LU 6.2 information.</p>

<b>Parameter</b>	<b>Description</b>
STARTT	<p>Specifies when NetSpy begins monitoring for alerts. Valid times include:</p> <ul style="list-style-type: none"><li>■ hh:mm</li><li>■ hh:mm:ss</li></ul> <p>STARTT defaults to 00:00:00.</p>
STOPT	<p>Specifies when NetSpy stops monitoring for alerts. Valid times include:</p> <ul style="list-style-type: none"><li>■ hh:mm</li><li>■ hh:mm:ss</li></ul> <p>STOPT defaults to 24:00:00. If you specify a start time and STOPT=99:99:99, monitoring runs continuously.</p>
TITLE	<p>Specifies the text associated with the monitor. You can specify up to 48 characters enclosed in single quotes. Indicate single quotes within the title with two single quotes, for example: TITLE='Alert Monitor for Bud''s Applications'</p>

# Installing the Unicenter Interface (Optional)

---

This chapter describes how to install the Unicenter Network Management Option, which is used to view your SNA configuration, NetSpy alerts, and historical reports from a Windows NT workstation running Unicenter SNA Manager Option.

For information on the installing the Unicenter Network Management Option for NetMaster, see the *Unicenter Network Management Option for NetMaster Getting Started* guide.

## Managing Your SNA Resources from a Workstation

NetSpy can act as an SNMP agent to send SNA configuration information and alerts to Unicenter (an SNMP manager). From a Windows NT workstation running Unicenter SNA Manager Option, you can do the following:

- View a graphical representation of your SNA resources on the Unicenter map
- View NetSpy alerts, whose severity is indicated by color, on the Unicenter map
- Launch NetSpy historical reports and information on alerts, in graphical and tabular format, from Unicenter

### CA-Datacom

To use NetSpy's Unicenter interface, you must install CA-Datacom. In addition to making NetSpy data accessible to Unicenter users, CA-Datacom provides you with powerful on demand reporting capabilities.

You can write reports against NetSpy historical data using software packages such as CA-Dataquery on the mainframe. On the PC, if you have the CA-Datacom Server installed, you have SQL access using an ODBC tool, such as CA-Visual Express.

## Establishing Communication with Unicenter

To install the Unicenter interface, perform the tasks described in this chapter.

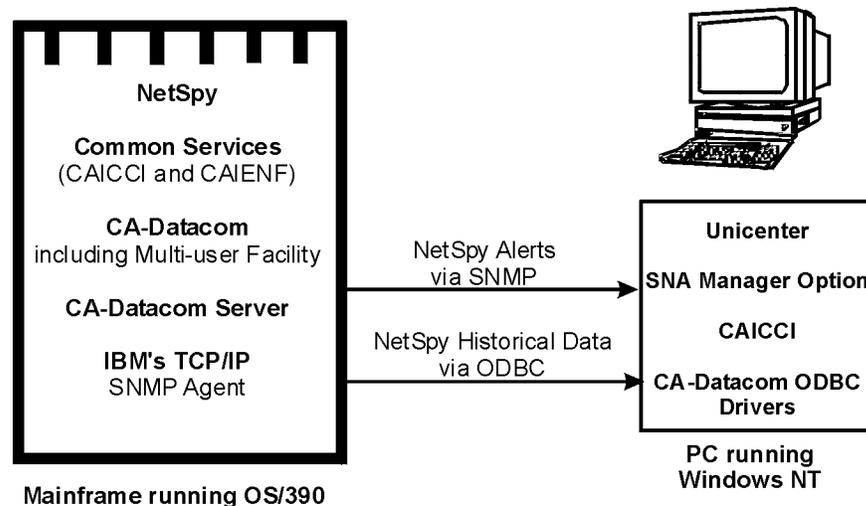
### Installing Required Software

**Step 1.** Install the following prerequisite software. Refer to the respective product documentation for instructions on installing these products.

1. The Unicenter Services for OS/390 and z/OS (any version). You must install the following components prior to installing CA-Datacom:
  - CAICCI
  - CAIENF
  - CAIRIM
2. CA-Datacom/AD or CA-Datacom/DB (version 8.1 or higher). The section [Notes on Installing CA-Datacom/AD](#) can assist you with the installation process. If the minimum required version of either of these products is already installed, the database required by NetSpy can be installed on the existing CA-Datacom installation.
3. CA-Datacom Server (version 3.0 or higher)

The following diagram provides an overview of the software that is required to establish communication between NetSpy on the mainframe and Unicenter on the workstation.

**Note:** NetSpy requires IBM's TCP/IP version 3.4 or higher with SNMP component.



## Allocating the Database

**Step 2.** Allocate the NetSpy Datacom Database. Follow these steps:

1. If you are running CA-Datcom 8.0 or 8.1, modify and submit the JCL in *dsnpref.NYvvv.CNTL(DBEXPAND)*. If you are running CA-Datcom 9.0 or above, this step is unnecessary.
2. Modify and submit the following JCL:
  - *dsnpref.NYvvv.CNTL(INSTDB)*, if using CA-Datcom/DB
  - *dsnpref.NYvvv.CNTL(INSTAD)*, if using CA-Datcom/AD

These jobs allocate the data sets for the database and run CA-Datcom utilities that prepare the data sets for use.

Instructions for modifying the JCL are provided in the member. If you are using CA-Datcom/DB, make sure you specify the three-digit Datacom database ID on the DBID parameter in member INSTDB. The default is 619 and should not be modified.

**Note:** Before submitting the job, make sure the CA-Datcom multi-user facility (DBMUF) is running.

*If You Encounter Errors When Running INSTDB or INSTAD* – If you are running CA-Datcom 8.0 or 8.1 and did not submit the DBEXPAND job prior to the INSTDB or INSTAD job, you will encounter errors. In this case, you can recover by submitting the JCL in *dsnpref.NYvvv.CNTL(DBDELETE)* to remove the partially installed NetSpy Database definitions. Then perform all the steps outlined in section [Allocating the Database](#). This step is not necessary for CA-Datcom 9.0 or above.

## Updating the Database When Upgrading

If you are upgrading to a new version of NetSpy in which the release notes state that new tables have been added to the database, and you already have the database defined, you must add the new tables to the existing database. Modify and submit the following JCL (instructions for modifying the JCL are provided in the member):

- *dsnpref.NYvvv.CNTL(UPDTDB)*, if using CA-Datcom/DB
- *dsnpref.NYvvv.CNTL(UPDTAD)*, if using CA-Datcom/AD

**Note:** The CA-Datcom multi-user facility (DBMUF) must be running.

The job that adds the new tables reinitializes the existing tables. If you want to retain the data in the database, use the instructions that follow.

**To Retain the Data in the Database**—If you want to retain the data in the database, do the following:

1. Before adding the new tables, run the NSYDBCX utility to convert the data to SMF records.
2. After running the job to add the new tables, run the NSYDBLD utility to load the SMF records into the database. The utility converts the data back to the database format.

## Modifying the NetSpy PROC

**Step 3.** Modify the NetSpy PROC.

The JCLPROC member of *dsnpref.NYvvv.CNTL* contains the necessary statements as comments to support database usage. Delete the comment characters and provide the appropriate data set names.

Refer to the JCLPROC member for instructions.

Submit the job to create the new PROC.

## Specifying IP Addresses

**Step 4.** Add the IP address of each Unicenter server that is to receive alerts from NetSpy to the *hlq.SNMPTRAP.DEST* data set. The format is:

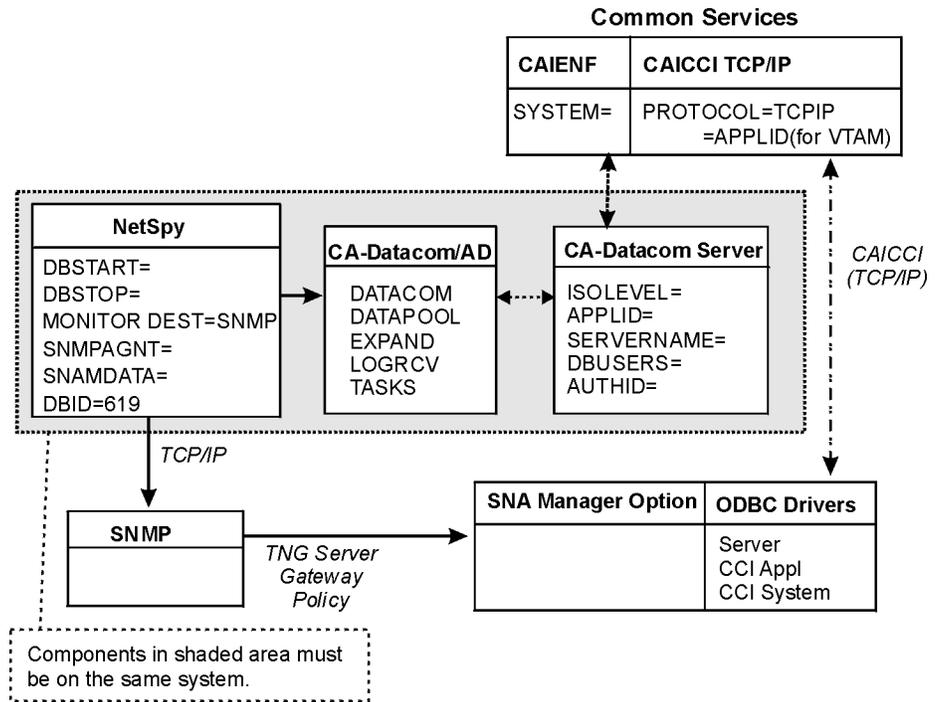
*ip.address* UDP

This parameter is part of the TCP/IP SNMP component, and can be defined in either a sequential data set, a member of a partitioned data set, or within OMVS's HFS file system.

## Customizing Settings

**Step 5.** Customize each component by specifying appropriate values on the required parameters.

The following diagram illustrates how the installed components are connected and the required parameters in each component. Use the diagram and the following tables to make sure the correct parameters correspond on the various components.



**Parameters Required for Setup**

Component	Parameter	Comment
Framework Common Services	SYSTEM= <i>sysname</i>	
CAIENF		
CAICCI/TCP	PROTOCOL=APPLID ( <i>for VTAM</i> )	The VTAM APPLID, for cross-OS/390 and z/OS systems only
	PROTOCOL=TCPIP	For Workstation communication
CA-Datacom	DATAKOM=DTCMSRVR	Identifies Datacom server to MUF
	DATAPOOL <i>dataIn,datano</i>	<i>dataIn</i> >=4K
	EXPAND <i>length,[number]</i>	<i>length</i> >=8K
	LOGRCV <i>entry</i>	<i>entry</i> =NO or NEVER
	TASKS <i>number,size</i>	<i>number</i> =1 + value of DBUSERS parameter on the Datacom server <i>size</i> =16K
		If other products are using the MUF in addition to NetSpy, you need to add the recommended number for those products also.
CA-Datacom Server	ISOLEVEL=U	No locks required, no changes are allowed
	APPLID= <i>applid</i>	
	SERVERNAME= <i>servername</i>	

	DBUSERS= <i>x</i>	The number of users to be viewing reports concurrently
	AUTHID=SYSUSR	
<b>NetSpy</b>		
INITPRM	DBSTART= <i>time</i>	To start logging NetSpy records to database
For details on defining NetSpy parameters, see the chapter entitled " <a href="#">Defining Initialization Parameters.</a> "	DBSTOP= <i>time</i>	Optionally, when to stop logging to database
	SNMPAGNT= <i>option</i>	Must match IP name of host running SNMP agent
	SNAMDATA= <i>option</i>	Location of NetSpy historical data
ALERTPRM	MONITOR DEST=SNMP	To send NetSpy alerts to Unicenter
DBPARMS	DBID=619	Datacom/AD uses default in INSTAD job. Datacom/DB uses the value set in INSTDB job; it must match the value in file DBPARMS pointed to in NetSpy PROC.

#### Corresponding Parameters Across Components

This Parameter...	on this component...	corresponds to this parameter...	on this component:
APPLID	CA-Datcom Server	CCI Appl	CA-Datcom ODBC Setup (Workstation)
SERVERNAME	CA-Datcom Server	SERVER	CA-Datcom ODBC Setup (Workstation)
SYSTEM	CAIENF	CCI System	CA-Datcom ODBC Setup (Workstation)
SNMPAGNT	NetSpy	TCP/IP name	Host running TCP/IP with SNMP component
SNAMDATA	NetSpy	CCI System ID	Host where historical data resides

## Notes on Installing CA-Datcom/AD

Detailed instructions for installing CA-Datcom/AD are provided in the CA-Datcom documentation. The purpose of this section is to point you to the essential instructions you need to install a new CA-Datcom/AD environment.

### Installing CA-Datcom/AD

When reading the installation instructions in the CA-DATACOM/AD documentation, you can ignore references to the following:

- Upgrading existing releases
- CA-DATAQUERY
- CICS services

Completing the Installation Work Sheet and Updating JCL

Use the installation work sheet provided in the *CA-DATACOM/AD* documentation. The work sheet lists the procedure parameters you should modify in the JCL for various installation steps. The parameters you must change are described below. The rest of the parameters are not used, so you can take their defaults.

Some of the parameters refer to libraries from prerequisite software. Make sure the prerequisite software listed in the Software Requirements section has been installed.

You must change (or review for accuracy) the following parameters:

- 1 through 7
- 10 through 29
- 36 through 39
- 41

**Note:** The documentation for this parameter is incorrect. If you are installing for the first time, you should use CAIMAC instead of INDSRC. Note that CAI.SHLQ is the same as parameter #1.

- 61 through 63

Running the Installation Jobs

When you are ready to run the installation jobs, you only need to perform installation phases 1, 2, and 4. Phases 1 and 2 consist of multiple steps each with a corresponding job that must be run. Do not run any steps that end in B, for example step 5B (job AXINS05B) of section 1.

It is recommended that you update your entire install JCL using the IPOUPDTE utility referred to in the “Pre-installation Considerations” section of the CA-DATACOM documentation. Do this after step 1 of the SMP/E Installation phase.

## Specifying Parameters for the Unicenter Interface

The following NetSpy statements and parameters (in the INITPRM, STARTPRM, and ALERTPRM files) pertain to the Unicenter interface. For details on each parameter, refer to the appropriate chapter in this manual.

File	Statement	Description
INITPRM	SNMPAGNT	Sends alerts and SNA configuration information to the Unicenter map
	CNFGITVL	Specifies how often SNA configuration

		information is refreshed
	SNAMDATA	Specifies the location of NetSpy data in a multiple NetSpy environment
	DBSTART	Writes data to the NetSpy Datacom Database
	DBSTOP	Stops writing data to the NetSpy Datacom Database
	RIFABNRM	Tailors NetSpy's reaction to a change in an alert's severity
	RIFNORM	Tailors NetSpy's reaction to a change in an alert's severity
STARTPRM	COLLECT	The LOG=DB operand on the COLLECT statement writes data to the NetSpy Datacom Database in a multiple NetSpy environment
	NETACCT	The ALOG=DB operand on the NETACCT statement logs network accounting statistics to the NetSpy Datacom Database
ALERTPRM	MONITOR	The DEST=SNMP operand on the MONITOR statement sends alert data to Unicenter's SNA manager option
		The DEST=DB operand on the MONITOR statement sends alert data to the NetSpy Datacom Database

## Using Cross-Communication to Map Your SNA Configuration

If you run multiple NetSpys, you can use NetSpy-to-NetSpy communication to map your SNA configuration.

### SNMPAGNT Parameter

By using a NetSpy-to-NetSpy link to one host that is running NetSpy and IBM's SNMP agent, you can consolidate all SNA configuration information on one system. (Without NetSpy-to-NetSpy communication, you would have to run an SNMP agent on every host that runs NetSpy.) This system then communicates with Unicenter to present a single map of SNA resources for the entire enterprise.

To use this feature, specify a value of REMOTE on the SNMPAGNT parameter in the INITPRM file.

**Note:** NetSpy-to-NetSpy support for SNA configuration mapping currently has the following limitations:

1. A copy of the NCP must be defined, but not acquired, on the local NetSpy.
2. Dynamic reconfiguration information is not sent NetSpy-to-NetSpy in the current version. Changes made by dynamic reconfiguration in an NCP that is being monitored by a NetSpy that is not directly communicating with Unicenter are not reflected on the map.

## Mapping Your SNA Configuration in a Multiple Host Environment

If you have a multiple host environment, the following customization tasks make it possible for you to view a single map of your SNA resources, as well as NetSpy historical data, from the Unicenter workstation.

You need to perform two general tasks:

1. Decide which NetSpys will communicate SNA configuration information to Unicenter.
2. Tell Unicenter where the historical data resides.

### Communicating SNA Configuration Information to Unicenter

NetSpy captures SNA configuration information for the host where it resides, its locally attached resources, and every NCP for which it is collecting data. When there is more than one SNA host in the network, you can obtain an integrated map using one of the following methods:

1. Use NetSpy-to-NetSpy communication to combine all data into a central NetSpy. The central NetSpy then communicates with Unicenter via the SNMP agent. This method requires you to:
  - a. Set up all NetSpys to communicate with the central NetSpy.
  - b. Specify the SNMPAGNT parameter on each NetSpy, as follows:
    - Central NetSpy: `SNMPAGNT=name`
    - NetSpy communicating with the central NetSpy:  
`SNMPAGNT=REMOTE`

2. Have each NetSpy communicate its own section of the map (which includes the host where it resides and the NCPs for which it collects data) to Unicenter via the SNMP agent. The workstation then integrates all views into a single map.

This method requires you to specify `SNMPAGENT=name` on each NetSpy.

3. Set up multiple central NetSpys to integrate separate map views and communicate with Unicenter. This is a combination of methods 1 and 2 above.

## Defining Historical Data to Unicenter

Another required task is to let Unicenter know where to find the historical data, so that it can display reports. The `SNAMDATA` parameter is used for this purpose. If there are several NetSpys communicating map information to Unicenter, you can use one of the following methods:

1. Have each NetSpy that communicates map information to Unicenter also communicate its historical data. In this case, you specify `SNAMDATA=LOCAL` for each one of those NetSpys.
2. Combine all historical data into one or more of the NetSpys that communicate with Unicenter.

In this case, for a NetSpy that communicates map information to Unicenter but stores historical data on another NetSpy, you specify `SNAMDATA=name`, where *name* is the CAICCI system ID for the host where the historical data resides. For the NetSpy where data resides, you specify `SNAMDATA=LOCAL`.

# Installing the Security Interface

---

NetSpy and NetMaster offer security interfaces that enable you to validate LOGON requests, so that only authorized users will be able to establish NetSpy sessions.

## Security Packages

NetSpy	In providing NetSpy's security interface, the user exit uses operating system services, the RACF, CA-Top Secret, or CA-ACF2, or a table of user IDs you specify.
NetMaster	See also the Security chapter of the <i>NetMaster for TCP/IP Administrator Guide</i> for information on installing and implementing security for the NetMaster product.

## RACF, CA-Top Secret, CA-ACF2

The *dsnpref.NYvvv.CNTL* data set has information about configuring the RACF, CA-Top Secret, and CA-ACF2 packages. The RACF, CA-Top Secret, and CA-ACF2 members provide sample user exits that you must customize for your site.

## SECURE Parameter

The control statement, `SECURE=YES`, is found in the initialization parameters and controls the execution of the security interface. It instructs NetSpy to call the security routine you provide each time a LOGON request is detected.

## User ID

The user ID must be either a valid security system user ID or a user ID defined within the internal table implemented when the security interface was installed. If the LOGON request does not belong to an authorized user, access is denied.

## Authorization Level

The exit may specify whether or not a user is authorized to execute all commands or only authorized to display information screens.

## Install the Security Interface

Follow the steps described in this section to install the security interface.

## File Contents

Use the members or files described here.

OS/390 and z/OS members	Description
NSYUPSWD	This is a sample interface that you must customize to your specific installation needs. The NSYUPSWD member can be found in the <i>dsnpref.NYvvv.CNTL</i> library.
SECURIN	This is a sample JCL stream that will assemble and link-edit the customized interface. The SECURIN member can be found in the <i>dsnpref.NYvvv.CNTL</i> library.

## Procedure

### Step 1 **Modify INITPRM to provide security control.**

Add the statement, SECURE=YES, to the initialization parameters (INITPRM) so that NetSpy will call the security exit every time it detects a LOGON request.

### Step 2 **Customize NSYUPSWD to suit your installation's needs.**

Edit the NSYUPSWD member to fit the requirements of your installation. You need to specify the environment in which NetSpy is running and the security options your site wants to use.

*To specify the OS/390 and z/OS system* in which NetSpy is running, use the following statement:

```
&ENV SETC MVS
```

To *provide security*, follow these steps:

1. Choose one of the following security options to check for a valid user ID.
  - You can have the program check a list of valid users from a built-in table that contains user IDs and corresponding passwords. To use this user list, before assembly, specify:

```
&MODE SETC LIST
```

- You can have the program access the operating system security interface through the RACF, CA-Top Secret, or CA-ACF2 macros and have your particular security system handle the LOGON authorizations.

To use the RACF or CA-Top Secret macros, before assembly, specify:

```
&MODE SETC RACF
```

To use the CA-ACF2 macro, before assembly, specify:

```
&MODE SETC ACF2
```

2. To indicate whether a valid user ID should be checked for authorization to log on to NetSpy specifically, specify one of the following statements:

```
&NSACCES SETC Y
&NSACCES SETC N
```

3. To determine whether or not a user who is logged on to NetSpy has authorization to issue all commands, specify one of the following statements:

```
&NSPRIV SETC Y
&NSPRIV SETC N
```

### User Exit Information

For the user exit to interrogate your security system and determine if a user is privileged to issue all NetSpy commands, the user record in the security system must identify the class of NetSpy user. The exit must then check this class and put a return code in R0 with one of the following values:

- 0 Privileged user. May execute all commands.
- 4 Normal user. May display only information screens.

With all options, the input parameters are as follows:

- R2 points to the user ID length (1 byte) followed by the user ID.
- R3 points to the password length (1 byte) followed by the password.
- R4 points to the new password length (1 byte) followed by the new password. This parameter is ignored with the built-in list.
- R9 points to the terminal name in an 8-byte field.
- R14 contains the return address.
- R15 contains the entry point.

Before returning to the calling program, the user exit must put a return code in R15 with one of the following values:

- 0 User is authorized, proceed with normal LOGON
- 4 User ID is invalid, terminate LOGON
- 8 Password is invalid, terminate LOGON
- 12 Password is expired, prompt for new password
- 16 User is not authorized to log on to NetSpy, terminate LOGON
- 24 New password was rejected by the security system
- 28 User ID is revoked

When using the security interface, consider these facts:

- R2 through R14 must be restored before returning to the calling program.
- OS/390 and z/OS Only: The exit runs as an authorized module under NetSpy's TCB (Task Control Block).
- The exit does not have to be reentrant.
- The exit must not issue implicit or explicit WAIT commands.

Step 3

**Complete the installation.**

Perform the following steps for an OS/390 and z/OS system.

**For OS/390 and z/OS: Customize and submit JCL in member SECURIN.**

Member SECURIN of *dsnpref.NYvvv.CNTL* contains sample JCL to assemble and link-edit the customized user exit into an APF-authorized library. Modify the JCL to point to the correct libraries at your installation and then submit it.

If you are assembling the security interface for use with CA-ACF2, do the following:

- Change the SYSLIB statement in the ASM step to reference the ACF2 macro library
- Change the SYSLIB statement in the LKED step to reference the ACF2 module library

# Generating NPA Support for Your NCPs

To generate NPA support for your NCPs you *must* include the statements in the following sections in each NCP for which NetSpy will be collecting data.

## The BUILD Definition Statement

The format of the BUILD definition statement is:

```
BUILD NPA=YES | (YES,DR)
[SESSACC=(YES,othervariables)]
[GWSESAC=(YES,othervariables)]
```

Note the following:

1. You must specify either the NPA=YES or the NPA=(YES,DR) parameters in the BUILD statement.

NetSpy supports the NCP option of providing dynamic reconfiguration information across the NCP's NPALU. When you specify NPA=(YES,DR) on the BUILD statement, the NCP sends an update of any dynamic reconfiguration of the network over the NPALU. NetSpy receives this information and updates the network and session statistics to reflect the dynamic changes in the network.

Use the NPA=(YES,DR) parameter when you want NetSpy to pick up NCP's dynamic reconfiguration resource information.

The DR option is also required for NetSpy to pick up token ring resources defined as switched nodes.

2. You must specify one of the NPA parameters and SESSACC=YES if you want to use network session accounting. If you specify SESSACC=YES without additional parameters, NetSpy uses the following defaults:

For NCP V5.4 and above: SESSACC=(YES,ALL,,25000,2500)

For NCP V4.3.1: SESSACC=(YES,ALL,,25000,2500,,(0))

In the default statements above:

- ALL** Specifies accounting on both PLU and SLU sessions.
- 25000** Specifies the byte threshold
- 2500** Specifies the PIU threshold
- 0** Specifies that no PIU distribution list is defined initially

If you do not want NetSpy to use these defaults, specify different values on the SESSACC=YES parameter in the NCP, or specify them in the NetSpy STARTPRM file or through NetSpy online menus.

3. To use network gateway accounting (with NCP V4.3.1), you must generate the NCP as a gateway NCP with the NPA=YES, SESSACC, and GWSESAC parameters. If no values are specified for these thresholds, NetSpy uses the following defaults:

```
SESSACC=(YES,ALL,,25000,2500,,(0))
GWSESAC=(YES,,,25000,2500,,0)
```

4. Line speeds in the NCP source must be correct for line utilization to be accurate.
5. If you are going to monitor NCPs, NetSpy's STEPLIB must refer to the same RRT that VTAM uses when activating the communication controller. Failure to do this will result in an error when NetSpy tries to establish a session with the NPALU. The library must be authorized in OS/390 and z/OS.
6. NPA=(YES,DRTP) is also a valid NCP definition.

## NPA Definition Statements

Include these statements:

```
npagrp GROUP VIRTUAL=YES,      Must be included in your stage 1
          LNCTL=SDLC,
          NPARSC=YES

npalne LINE
npapu  PU
npalu  LU   [MAXCOLL=nn]      Default=number of lines + 10
                               (For NCP V4.3/5.2 and above, the
                               default is all NPA collectable
                               devices.)

                               [LOGAPPL=applid]
```

Note the following:

1. Only one application can be in session with the NPALU at a time.
2. The MAXCOLL parameter defines the number of resources for which data collection buffers will be allocated in the NCP (the maximum number of resources for which NPA data can be collected). The number of bytes of NCP buffer space used for each increment of this value is 104 (40 bytes for NCP V5.4 and above).
3. The MAXCOLL parameter must not be set larger than the number of eligible devices in the NCP.
4. MAXCOLL is an NCP parameter, and if changed, the NCP must be regenerated.
5. You can specify the NPALU with the LOGAPPL parameter so that when the NCP is activated, a session between NetSpy and the NPALU will automatically start without operator intervention.

Include these statements:

GROUP NPACOLL=YES LINE CLUSTER TERMINAL	Must be specified or defaulted for the elements for which you want to collect statistics.  Default for SDLC lines is NPACOLL=YES.
--	---

Note the following:

1. The GROUP statement trickles the NPACOLL parameter down to subordinate resources.
2. You should monitor both LINES and PUS by specifying them on the SCOPE parameter of the SSMF command in member STARTPRM. You may want to allow a few extra resources on MAXCOLL to monitor a terminal in a problem situation.
3. X.25 lines are monitored by NetSpy when NPA data is collected from NCP V5.4 and NPSI V3.4. (NPA data collected from previous versions is not accurate.)  
  
The NPACOLL statement must be specified in the NCP generation in order to monitor X.25 resources. To do this, specify  
NPACOLL=(MCHLINE,MCHPU,VCPU) on the X25.MCH macro.
4. The only bisynchronous devices supported for NPA collection in an NCP are BSC 327x-type clusters.
5. For BSC devices, you must specify NPACOLL=YES to collect NPA data.

For complete details on generating NPA support for X.25 resources, refer to IBM's NPSI installation manual.

## Troubleshooting

If you have problems getting the NCP interface to function, check the following:

- Is the NetSpy region size too small? Check for NetSpy or system error messages relating to storage shortages.
- Is the VERSION parameter in the BUILD macro correct?
- Does STEPLIB contain the correct NCP library?
- Has a new generation been performed lately and not loaded?
- Has the NCP source code in SYS1.VTAMLST for OS/390 and z/OS been changed?
- Is the NPALU defined?
- Was NPA=YES or NPA=(YES,DR) specified in the BUILD statement?
- Is the NPALU already in session with another application?
- Has MAXCOLL been updated but the NCP not generated with this update?

# Activating the Unicenter Performance Management Predictor Option

NetSpy performance data is now available to Neugents through the Unicenter Performance Management Predictor interface. You can provide NetSpy data to the Unicenter Performance Management Predictor by:

- Setting the INITPRM member to activate the real time interface.
- Running the NSYNHIST program for historical data

## Initialization Parameters

The initialization parameters are read from the INITPRM member of the *dsnpref.NYvvv.CNTL* partitioned data set (identified on the //INITPRM DD statement in the startup PROC). See the chapter “[Defining Initialization Parameters](#)” for additional information.

### NEUPERF Parameter

This statement activates or inactivates the real time interface to the Unicenter Performance Management Predictor.

```
NEUPERF=OFF  
NEUPERF=ON  ENTITY=entity SSN=ssn FILTWARN=YES|NO  ERRLLIM=9999999  
            OTHERSYS=INCLUDE|EXCLUDE  RECORDS=recordtypes
```

NEUPERF=OFF turns off the interface to the Unicenter Performance Management Predictor and is the default.

NEUPERF=ON turns on the interface to the Unicenter Performance Management Predictor, which will activate the other parameters.

The following parameters only have meaning if NEUPERF=ON is coded:

Parameter	Explanation
ENTITY= <i>entity</i>	Specifies a one to eight character entity name to be passed to the Unicenter Performance Management Predictor External Data Interface. This value shows up as the <i>session name</i> on Performance Management Predictor displays.  Default is NSYMAIN
ERRLIM= 9999999	Specifies a one to seven digit maximum number of error messages written to the console that reports non-zero return codes from the Unicenter Performance Management Predictor External Data Interface. When the specified number of messages has been written, future errors are not reported.  Default is 10.
FILTWARN= YES or NO	Specifies whether to produce the NSY2103 error message on the console when filtering rejects the data presented to the Unicenter Performance Management Predictor External Data Interface.  Default is NO
OTHERSYS= INCLUDE or EXCLUDE	Specifies which log records collected from other systems are to be passed to the Unicenter Performance Management Predictor External Data Interface. INCLUDE indicates all records will be passed, and EXCLUDE indicates only records created in this NetSpy system will be passed.  Default is INCLUDE
RECORDS= <i>recordtype</i>	Indicates which record types will be passed to the Unicenter Performance Management Predictor External Data Interface. Specify either ALL, for every record type, or a string of characters separated by commas and enclosed in parenthesis. List the record types as defined in the chapter "Log Record Layouts."  Example: RECORDS=(A,B,V)  Default is ALL
SSN= <i>ssn</i>	Specifies the one to four character subsystem name for the Unicenter Performance Management Predictor External Data Interface.  Default is NEUP.

See the NEUPDOC member in *dsnpref.NYvvv.CNTL* for details about variable names.

## JCL for NSYNHIST

NSYNHIST is a batch program that can be used to pass large amounts of historical data, in the form of NetSpy log records, to the Unicenter Performance Management Predictor. Use the following JCL to run the NSYNHIST program:

```
//STEPX   EXEC   PGM=NSYNHIST,
//          PARM='SIMULATE' ,
//          REGION=0M
//STEPLIB DD    DSN=netspy.loadlib,
//          DISP=SHR
//SYSPRINT DD   SYSOUT=*
//NSYLOG  DD    DSN=netspy.logdump,
//          DISP=SHR
//SYSIN   DD    *
           control statements
```

Omit the PARM field when the data is to be passed to the Unicenter Performance Management Predictor interface.

When PARM='SIMULATE' is specified, no data is passed to the interface. This feature provides a report listing the number of records that would be processed by the Unicenter Performance Management Predictor in an actual run.

## Control Statements

This section explains each control statement.

### ENTITY=*entity*

*entity* specifies a 1 to 8 character entity name to be passed to the Unicenter Performance Management Predictor External Data Interface. The default is NSYMAIN.

### ERRLIM=9999999

9999999 specifies a 1 to 7 digit maximum number of error messages written to the console reporting non-zero return codes from the Unicenter Performance Management Predictor External Data Interface. After the specified maximum number of messages are written, future errors are not reported. The default is 10.

### EXCLUDE=(*smf1,smf2,smf3,...smfn*)

*smf1,smf2,smf3...smfn* specify the 1 to 4 character SMF IDs associated with log records that are not to be passed to the Unicenter Performance Management Predictor External Data Interface. If there is only one SMF ID in the list, the parentheses are not needed. The default is to pass data for every SMF ID.

### **FILTWARN=YES | NO**

YES or NO specifies whether or not to produce the NSY2103 error message on the console when filtering rejects the data presented to the Unicenter Performance Management Predictor External Data Interface. The default is NO.

### **RECORDS=recordtypes**

*recordtypes* indicates which record types are passed to the Unicenter Performance Management Predictor External Data Interface. Specify either ALL, for every record type, or a string of characters separated by commas and enclosed in parenthesis. List the record types, as defined in the chapter “[Log Record Layouts](#)”. The default is ALL.

Example: RECORDS=(A,B,V)

### **SMF#=nnn**

*nnn* specifies the SMF record number between 0 and 255 used to collect NetSpy records at your installation. This value must match the value set on the SMF, the LOGTYPE, or both parameters in your NetSpy INITPRM member.

### **SSN=ssn**

*ssn* specifies the 1 to 4 character subsystem name for the Unicenter Performance Management Predictor External Data Interface. The default is NEUP.

See the Unicenter Performance Management Predictor for z/OS and OS/390 documentation for more information about setting up the subsystem.

# Installing a Session Manager Interface

---

For more specific instructions on the installation of and interface with the session managers, contact your session manager vendor.

## Session Managers Supported

The following session managers provide support for a NetSpy interface:

- CA-TPX
- CA-Teleview
- Multsess
- CL/Supersession
- NetMaster
- Net-Pass
- VTAM/Switch
- VTAM/Tubes
- Intersess
- BiWindow
- NetGate (PI/CICS)

If you use one of these session managers, NetSpy provides an interface to report all network statistics for the real terminals. Without this interface, when a terminal accesses an application via the session manager, NetSpy provides the proper host and network times for the session manager session only.

However, with the session manager interface installed, NetSpy will report complete statistics for all those sessions established through the session manager. The interface is implemented by having the session manager notify NetSpy whenever there is a new session startup or a session switch. NetSpy uses this information to correlate the terminal statistics with the real application with which it is in session at the time.

## How to Install a Session Manager Interface

Follow the procedure below to install a session manager interface.

1. **Use real VTAM application names.**

Be sure that only real VTAM application names are specified in the application definitions of the session manager. ACBNAMEs will work in these definitions for any session manager, but the NetSpy interface will not work correctly unless real network names are used.

2. **Make all the following modifications on the OS/390 and z/OS system.**

Modify your INITPRM member to support the session manager/NetSpy interface as follows. INITPRM contains sample definitions for a session manager environment.

- a. Place the APPLNAME=NETNAME statement before all APPL statements.
- b. Place all other parameter statements before the APPL statements.
- c. Change all APPL statements to specify the real network name instead of the ACBNAME. You may add cross-domain applications that will be accessed from the session manager. These applications can be monitored in conjunction with a session manager only. This is the only case where NetSpy will monitor applications in another host.
- d. Specify SMANAGER=name on the session manager APPL statement.
- e. Specify FORCEDR=100 on the session manager APPL statement.
- f. Use the ALIAS parameter instead of "(n)" for applications like TSO and NCCF that have subapplications defined in VTAM.
- g. Do not specify the TARGET parameters for the session manager APPL statement. Targets will be reported for other application sessions on behalf of the real terminal. Because the session manager is just a medium for communicating with an application, the targets can vary according to the application with which the terminal is in session.

3. **Call your session manager provider for the latest fixes.**

### For CA-TPX Users Only

If you are using CA-TPX 4.1 or above do the following:

1. Access the CA-TPX administrator.
2. Select System Options from the menu.
3. Select System Features and specify Y to activate the NetSpy interface. If you want to turn off the interface, specify N.

## Test the interface

You will know the exit is working when you see V-LU in the last column of the terminal display (PF6) and the physical terminal name appears instead of the virtual terminal name.

## For CA-Teleview Users Only

If you are using any CA-Teleview release earlier than 4.3, genlevel 9905, do the following:

1. Read the NSYSMGRI information member in *dsnpref.NYvvv.CNTL*.
2. Implement the NSYSMGRX exit found in the same library.



# Creating and Enabling the NetView Interface

You can route NetSpy general alerts to NetView Version 3 Release 0 or higher.

## Create a Startup Procedure for NetView

If your system contains the NetView program Version 3 Release 0 or higher, you can route general alerts to it by putting the NetView program-to-program interface in the CNMLINK data set and adding the following statement to the STEPLIB concatenation of your NetSpy startup procedure:

```
// DD DSN=SYS1.CNMLINK,DISP=SHR
```

The name SYS1.CNMLINK may differ in your particular installation. If you omit the above statement, or if your version of NetView is lower than 3.0, you will see the following message on your system console when you start up NetSpy:

```
NSY3313 - LOAD FAILED FOR CNMNETV - NETSPY ALERTS WILL NOT BE SENT TO NETVIEW
```

In the message above, CNMNETV is an alias for CNMCNETV.

## Steps to Enable the Interface

NetSpy supports the NetView interface for OS/390 and z/OS. Note that the following information is reprinted by permission from *NetView Application Programming: Program-to-Program Interface* (SC31-6093-0) copyright 1989 by International Business Machines Corporation.

To enable the program-to-program interface, do the following:

1. Make sure that the NetView communication network management task, DSICRTR, is active. To find the status of this task, issue the command LIST DSICRTR from the NetView command line.
  - If the status is ACTIVE, proceed to step 3.
  - If the status is INACTIVE, issue the command START TASK=DSICRTR.

2. Ensure that the NetView alert receiver task, CNMCALRT, is defined to NetView and is started when NetView is brought up. To find the status of this task, issue the command LIST CNMCALRT from the NetView command line.

- If the status is ACTIVE, proceed to step 4.
- If the status is INACTIVE, issue the command START TASK=CNMCALRT.
- If the response from NetView is this message:  
DSI077A 'CNMCALRT' STATION NAME UNKNOWN

add the following task statement to the NetView member DSIDMN:

```
TASK MOD=CNMCALRT, TSKID=CNMCALRT, PRI=6, INIT=Y
```

The priority for this task should be the same as the priority for the DSICRTR task.

**Note:** NetView must be restarted after the task statement is added.

3. Make sure that the subsystem name for the NetView subsystem address space is a subsystem name entry in the OS/390 and z/OS subsystem name table (IEFSSNxx) in SYS1.PARMLIB.

When multiple NetView subsystem address spaces are active, the address space specified first in the OS/390 and z/OS subsystem name table will process requests sent across the interface. Refer to the IBM document, *OS/390 MVS Initialization and Tuning Reference*, for more information about the subsystem name table.

4. Ensure that the NetView subsystem address space has a specified region size large enough to hold the user data buffers that might be queued or stored in the subsystem address space.

The required storage depends on how many receivers exist in the NetView subsystem address space. To estimate the required storage, perform the following steps:

- a. Determine the storage required for each receiver:

Average buffer size x buffer queue limit  
(bytes) (number of buffers)

- b. Add the storage requirements for all the receivers to get an estimate of total storage required, in bytes.

## NetView Return Codes

The following table describes the NetView return codes NetSpy issues in error messages.

<b>Code</b>	<b>Description</b>
0	The request completed successfully.
4	The NetView alert receiver task is inactive. The NetView subsystem has received a copy of the alert buffer.
22	The program issuing this request is not executing in primary addressing mode.
24	The NetView subsystem is not active.
26	The alert receiver task is not defined.
28	This NetView release does not support user requests.
32	No NetView storage is available.
33	Invalid buffer length.
35	The alert receiver buffer queue is full.
36	ESTAE recovery cannot be established as requested.
40	Invalid SENDER-ID.
90	A processing error has occurred.



NetSpy writes log records that serve as input to the batch reporting system.

## Log Record Types

The NetSpy log records use an SMF format, with fixed SMF headers and variable SMF data sections. The size of the variable section depends on the record type.

There are several log record types:

Record	Type	When Written
Application	Type A	Each interval
VTAM buffer	Type B	Each interval
Network accounting	Type C	Each base interval
APPN directory services	Type D	Each interval
MNPS application recovery	Type E	Each interval
MNPS coupling facility structure	Type F	Each interval
TCP/IP UDP connections	Type G	Each interval
TCP/IP interface	Type H	Each interval
TCP/IP TCP connections	Type I	Each interval
TCP/IP stack	Type J	Each interval
MNPS application	Type M	Each interval
NCP	Type N	Each interval
APPN topology	Type P	Each interval
VTAM RTP	Type R	Each interval
Session	Type S*	When a session is initiated or terminated
Terminal	Types T and U	Each interval (type T) and each base interval (type U)
Virtual route	Type V	Each interval

General alert	Type X	Each interval in which a general alert occurred or when the logging I/O buffer is full
---------------	--------	--

\*Type S log records are written only to SMF, not to the Log or Database.

## SMF Record Header

The first 90 bytes of each log record contain the SMF header described in the table below.

Length	Offset (in decimal)	Type	Description
4	0	N	Record descriptor word (RDW)
14	4	N	Standard SMF record header:
1	4	N	■ Flag byte
1	5	N	■ SMF record type
4	6	N	■ TOD (hundredths of seconds since midnight)
4	10	N	■ Date (packed decimal form: 00yydddff)*
4	14	C	■ System identification
			*A non-zero value in place of 00 indicates a 21st century date
1	18	C	NetSpy record subtype:
			■ For application, A
			■ For VTAM buffer, B
			■ For network accounting, C
			■ For APPN directory services, D
			■ For MNPS application recovery, E
			■ For MNPS coupling facility structure, F
			■ For Telnet connected LUs, I
			■ For TCP/IP stack statistics, J
			■ For MNPS application, M
			■ For NCP element, N
			■ For APPN topology, P
			■ For VTAM RTP data, R
			■ For session, S
			■ For terminal, T or U

Length	Offset (in decimal)	Type	Description
			<ul style="list-style-type: none"> <li>■ For virtual route, V</li> <li>■ For general alert, X</li> </ul>
1	19	N	Number of entries for record
2	20	N	Length of entry
8	22	C	Major resource name, if applicable: <ul style="list-style-type: none"> <li>■ For A entries, binary zeros</li> <li>■ For B and C entries, NCP Name</li> <li>■ For D entries, binary zeros</li> <li>■ For E entries, binary zeros</li> <li>■ For F entries, binary zeros</li> <li>■ For J entries, binary zeros</li> <li>■ For M entries, binary zeros</li> <li>■ For N entries, NCP name</li> <li>■ For P entries, binary zeros</li> <li>■ For R entries, binary zeros</li> <li>■ For I, S, T, and U entries: application name</li> <li>■ For V entries, the first four bytes of the host subarea number</li> <li>■ For X entries, binary zeros</li> </ul>
4	30	N	Interval length (in hundredths of seconds)
1	34	C	Zero
3	35	C	Reserved
4	38	N	Offset from the beginning of the RDW to the first entry
4	42	C	The NetSpy release from which the data in this record originated (in format <i>rn.n</i> , for example, r4.7)
4	46	N	SYNC parameter (in hundredths of seconds)

**Note:** The byte values described below apply *only* to type C, S, T, and U entries. For all other entries (except type C entries), these bytes are set to all zeros. If the entry is type C, the following byte entries contain network accounting PIU distribution ranges.

1	50	N	Flag: <ul style="list-style-type: none"> <li>■ If UTARGETs (USER targets) are defined, X'80' bit</li> <li>■ If NTARGETs (NET targets) are defined, X'40' bit</li> <li>■ If HTARGETs (host targets) are defined, X'20' bit</li> <li>=0 if user time is defined (0 is the default)</li> <li>=1 if host time is defined</li> </ul>
---	----	---	---

Length	Offset (in decimal)	Type	Description
			<ul style="list-style-type: none"> <li>■ If type C entry, X'10' bit, PIU distribution ranges follow</li> <li>■ If type I entry: <ul style="list-style-type: none"> <li>X'80' bit, interval record</li> <li>X'40' bit, final record for ended session</li> </ul> </li> </ul>
1	51	C	Reserved
2	52	N	APPL target level 1 (in 2 <sup>16</sup> microseconds) <i>or</i> if type C, PIU distribution range 1
2	54	N	APPL target level 2 (in 2 <sup>16</sup> microseconds) <i>or</i> if type C, PIU distribution range 2
2	56	N	APPL target level 3 (in 2 <sup>16</sup> microseconds) <i>or</i> if type C, PIU distribution range 3
2	58	N	APPL target level 4 (in 2 <sup>16</sup> microseconds) <i>or</i> if type C, PIU distribution range 4
2	60	N	USER/NET target level 1 (in 2 <sup>16</sup> microseconds) <i>or</i> if type C, PIU distribution range 5
2	62	N	USER/NET target level 2 (in 2 <sup>16</sup> microseconds) <i>or</i> if type C, PIU distribution range 6
2	64	N	USER/NET target level 3 (in 2 <sup>16</sup> microseconds)
2	66	N	USER/NET target level 4 (in 2 <sup>16</sup> microseconds)
2	68	N	Reserved
4	70	N	Reserved
8	74	N	Network ID
8	82	N	Reserved

## Type A (Application) Entry

The table below describes type A entries, which contain 340 bytes and supply information about the applications that NetSpy was monitoring at interval end. *Type A is the only entry that contains both target values and counts. If target values are not specified, their corresponding target counts are set to zero.*

Length	Offset	Type	Description
8	0	C	Application name
4	8	N	Application CID (network address)
<i>Non-LU 6.2 session information:</i>			
4	12	N	Last host response time (in $2^{16}$ microseconds)
4	16	N	Last network response time (in $2^{16}$ microseconds)
4	20	N	Worst host response time (in $2^{16}$ microseconds)
4	24	N	Worst network response time (in $2^{16}$ microseconds)
4	28	N	Cumulative host response time (in $2^{16}$ microseconds)
4	32	N	Cumulative network response time (in $2^{16}$ microseconds)
4	36	N	Number of inputs (initiated transactions)
4	40	N	Number of outputs
4	44	N	Number of network responses computed
4	48	N	Number of transactions terminated at the host
4	52	N	Number of responses on target 1
8	56	N	Cumulative inbound bytes
8	64	N	Cumulative outbound bytes
36	72	C	Reserved
4	108	N	Number of active sessions at end of interval
<i>For both LU 6.2 and non-LU 6.2 sessions:</i>			
4	112	N	Target level 1 (in $2^{16}$ microseconds)
4	116	N	Target level 2 (in $2^{16}$ microseconds)
4	120	N	Target level 3 (in $2^{16}$ microseconds)
4	124	N	Target level 4 (in $2^{16}$ microseconds)
<i>For non-LU 6.2 sessions:</i>			
4	128	N	Number of responses on target 2

Length	Offset	Type	Description
4	132	N	Number of responses on target 3
4	136	N	Number of responses on target 4
<i>For both LU 6.2 and non-LU 6.2 sessions:</i>			
2	140	N	Max number of terminals that can be monitored for this application (as specified in the MAXLU parameter). Defaults to 65,535.
3	142	C	Reserved
1	145	N	Application flag: <ul style="list-style-type: none"> <li>■ If targets are computed on host response only, X'40' bit</li> <li>■ If it is a session manager application, X'20' bit</li> <li>■ If it is a cross-domain application, X'10' bit</li> </ul>
8	146	C	Reserved
1	154	N	Resource type flag: X'08' bit <ul style="list-style-type: none"> <li>■ If X'08' is off, resource is a real VTAM application</li> <li>■ If X'08' is on, resource is a transaction group</li> </ul>
29	155	C	Reserved
8	184	N	Number of bytes sent outbound on sessions where response times are not being monitored

**Note:** The field at offset 184 contains the total number of bytes sent outbound on sessions within the interval. The number of outbound bytes on these sessions is also included in the “cumulative output length” field at decimal offset 64. Subtracting the byte count field at offset 184 from the cumulative output length field gives you the total number of outbound bytes on sessions where response times and transactions are being monitored. This field is an 8-byte unsigned binary field similar to the one found at decimal offset 64.

*LU 6.2 session information:*

4	192	N	Number of transactions (Attaches) initiated on LU 6.2 sessions
4	196	N	Worst host response time for any LU 6.2 session (in $2^{16}$ microseconds)
4	200	N	Worst network response time (in $2^{16}$ microseconds)
4	204	N	Cumulative host response time for all sessions (in $2^{16}$ microseconds)
4	208	N	Cumulative network response time for all sessions (in $2^{16}$ microseconds)
4	212	N	Number of inputs for all sessions
4	216	N	Number of outputs for all sessions
4	220	N	Number of network responses for all sessions
4	224	N	Number of transactions measured at the host for all sessions

Length	Offset	Type	Description
8	228	N	Cumulative inbound bytes for all sessions
8	236	N	Cumulative outbound bytes for all sessions
4	244	N	Number of active sessions at end of interval
4	248	N	Number of responses on target 1 for all sessions
4	252	N	Number of responses on target 2 for all sessions
4	256	N	Number of responses on target 3 for all sessions
4	260	N	Number of responses on target 4 for all sessions
4	264	N	Number of user responses
8	268	N	Network ID of the application (ESA only)
64	276	N	Reserved

## Type B (VTAM Buffer) Entry

Type B entries for VTAM buffer statistics records are described in the table below. These entries contain 64 bytes.

Length	Offset	Type	Description
4	0	C	Buffer pool ID
4	4	C	Blanks
4	8	N	Base allocation (NUM + NUMR) of buffers at VTAM initialization
4	12	N	Total number of buffers (allocated + unallocated) currently in static and expanded pools since last SMS record was written*
4	16	N	Total number of buffers currently in use since last SMS record was written*
4	20	N	Total number of buffers currently available in static and expanded areas
4	24	N	Total number of buffers currently in the static area
2	28	N	Slowdown threshold
2	30	N	Expansion threshold in number of buffers (or x 'FFFF' if not eligible)
4	32	N	Number of buffers over the slowdown point
4	36	N	Number of buffers over the expansion point
4	40	N	Maximum number of buffers allocated since last SMS record was written*

Length	Offset	Type	Description
4	44	N	Maximum number of buffers in use since last SMS record was written*
2	48	N	Expansion increment in number of buffers
2	50	N	Contraction threshold in number of buffers (or x '7FFF' if no expansion extents yet)
4	52	N	Number of times pool expanded since last SMS record was written*
4	56	N	Number of active extents
2	60	N	Size of buffers in the buffer pool
2	62	N	Reserved

**Note:** \*SMS records are written if the VTAM trace is active on the system. If a trace is not active, the number of buffers since the VTAM initialization is counted.

## Type C (Network Accounting) Entry

Type C records, described in the table below, contain 288 bytes and supply network accounting information about NCP sessions.

Type C records are optional. To collect them, either specify the NETACCT statement in the STARTPRM member, or select the network accounting option on the Operator Command Menu.

Type C records are written to SMF, the Log, or Database, depending on the value of the ALOG parameter on the NETACCT statement in the STARTPRM file, or the Start Network Accounting Display screen.

Length	Offset	Type	Description
1	0	C	Type of session record: <ul style="list-style-type: none"> <li>■ For session start record, S</li> <li>■ For session interval record, I</li> <li>■ For session end record, E</li> </ul>
1	1	C	Type of network accounting record <ul style="list-style-type: none"> <li>■ For gateway, G</li> <li>■ For network, N</li> </ul>
4	2	P	Session start date (in packed decimal form 00yydddf)
4	6	N	Session start time (hundredths of seconds since midnight)

Length	Offset	Type	Description
8	10	C	Session LU name
6	18	N	Session LU network address:
4		N	Session LU subarea address
2		N	Session LU element address
2	24	B	Sequence number for this session
8	26	C	Session partner network ID
8	34	C	Session partner name
6	42	N	Session SPLU network address:
4		N	Session SPLU subarea address
2		N	Session SPLU element address
8	48	C	Line name
6	56	N	Line address:
4		N	Subarea address
2		N	Element address
8	62	C	Link station name
6	70	N	Link station network address:
4		N	Subarea address
2		N	Element address
8	76	C	NCP of this LU
4	84	N	NCP subarea
8	88	C	Network ID for the LU
17	96	C	CP qualified name
1	113	B	Virtual route number
1	114	B	Transmission priority
1	115	B	Explicit route
1	116	B	Reverse ER data
1	117	B	FID type
1	118	B	Local origin address
1	119	B	Local destination address
4	120	P	Session stop date/interval date (in packed decimal form 00yydddff)

Length	Offset	Type	Description
4	124	N	Session stop time/interval time (hundredths of seconds since midnight)
4	128	B	Total text PIUs received
4	132	B	Total text PIUs sent
4	136	B	Total text bytes received
4	140	B	Total text bytes sent
4	144	B	Total control PIUs received
4	148	B	Total control PIUs sent
4	152	B	Total control bytes received
4	156	B	Total control bytes sent
1	160	B	Overflow counter for PIUs text received
1	161	B	Overflow counter for PIUs text sent
1	162	B	Overflow counter for byte text received
1	163	B	Overflow counter for byte text sent
1	164	B	Overflow counter for PIUs control received
1	165	B	Overflow counter for PIUs control sent
1	166	B	Overflow counter for byte control received
1	167	B	Overflow counter for byte control sent
8	168	C	Adjacent network ID of SLU (GWA)
8	176	C	Adjacent network ID of PLU (GWA)
4	184	B	Total PIUs received in distribution range 1
4	188	B	Total PIUs received in distribution range 2
4	192	B	Total PIUs received in distribution range 3
4	196	B	Total PIUs received in distribution range 4
4	200	B	Total PIUs received in distribution range 5
4	204	B	Total PIUs received in distribution range 6
4	208	B	Total PIUs received in distribution range 7
4	212	B	Total PIUs sent in distribution range 1
4	216	B	Total PIUs sent in distribution range 2
4	220	B	Total PIUs sent in distribution range 3
4	224	B	Total PIUs sent in distribution range 4

Length	Offset	Type	Description
4	228	B	Total PIUs sent in distribution range 5
4	232	B	Total PIUs sent in distribution range 6
4	236	B	Total PIUs sent in distribution range 7
14	240	B	PIU distribution overflow bytes:
7		B	For receive byte ranges 1-7
7		B	For send byte ranges 1-7
1	254	C	Session start record status: <ul style="list-style-type: none"> <li>■ C indicates that the session start record was written</li> <li>■ I indicates that the session start record was not written</li> <li>■ R indicates that all counters have been reset relative to 0.</li> </ul>
1	255	B	Session flags: <ul style="list-style-type: none"> <li>■ If the LU is primary for session, X'80' bit</li> <li>■ If the SNI date/time session is included, X'10' bit</li> <li>■ If the FID ODA is from the transmission header (TH) of the BIND, X'40' bit</li> <li>■ If the boundary is LU-LU, X'n0' bits</li> <li>■ If the gateway is LU-LU, X'n1' bits</li> <li>■ If the gateway is SSCP-SSCP, X'n2' bits</li> <li>■ If the gateway is FID0, X'n3' bits</li> </ul>
8	256	C	Alias name of SLU (GWA)
8	264	C	Alias name of PLU (GWA)
8	272	C	NCP-PCID session ID value
8	280	C	SNI date/time if available

## Type D (APPN Directory Services) Entry

Type D entries for APPN Directory Services records are described in the table below. These entries contain 64 bytes.

<b>Length</b>	<b>Offset</b>	<b>Type</b>	<b>Description</b>
4	0	N	Number of resources successfully found in local database cache
4	4	N	Number of resources successfully found from the central directory server
4	8	N	Number of resources successfully found via domain broadcast
4	12	N	Number of resources successfully found via network broadcast
4	16	N	Number of failed searches completed by receipt of a negative reply
4	20	N	Number of times a network broadcast is not performed due to a negative cache entry
4	24	N	Number of matches where this node received a search request from another node and the requested resource was found
4	28	N	Number of matches where this node received a search request from another node and the requested resource was not found
4	32	N	Number of referrals received
4	36	N	Number of times a positive reply is received from an alternate central directory server
4	40	N	Number of times a negative reply is received from an alternate central directory server
4	44	N	Number of resources removed from local database due to value specified for either the DIRSIZE or DIRTIME start options
4	48	N	Number of adjacent nodes in a different sub-network
4	52	N	Number of times a cache entry is discarded due to DIRSIZE maximum being reached
4	56	N	Number of registered resources
4	60	N	Current number of entries in the cache

## Type E (MNPS Application Recovery) Entry

Type E entries for MNPS application records are described in the table below. These entries contain 32 bytes.

Length	Offset	Type	Description
8	0	C	Application program name
4	8	N	Number of sessions recovered successfully by this VTAM
4	12	N	Number of session recoveries attempted
4	16	N	Number of HPR pipes recovered successfully by this VTAM
4	20	N	Number of HPR pipes recoveries attempted
8	24	N	Total recovery time spent recovering sessions (TOD clock format)

## Type F (MNPS Coupling Facility Structure) Entry

Type F entries for MNPS coupling facility records are described in the table below. These entries contain 24 bytes.

Length	Offset	Type	Description
16	0	C	Coupling facility structure name
4	16	N	Coupling facility structure size in 1K blocks
4	20	C	Percentage of 1K blocks in use

## Type G (UDP Connection) Entry

Type G records are TCP/IP UDP connection records, written each interval when UDP collection and logging is turned on. UDP=(Y,Y)

Fields are stack type specific. All fields are available for IBM type stacks unless indicated otherwise.

Length	Offset (hex)	Type	Description
16	000000	C	Connection local address (stack type = I/O)
6	000010	C	Connection local port (stack type = I/O)

Length	Offset (hex)	Type	Description
8	000018	C	Resource name
8	000020	C	Resource ID
8	000028	C	Subtask
4	000030	N	Last activity
4	000034	N	Send limit
4	000038	N	Receive limit
4	00003C	N	Datagram in
4	000040	N	Datagram out
4	000044	N	Bytes out
4	000048	N	Bytes in

## Type H (Interface) Entry

Type H records are TCP/IP interface records, written each interval when IF collection and logging is turned on. IF=(Y,Y)

Fields are stack type specific. All fields are available for both IBM or Other type stacks.

Length	Offset (hex)	Type	Description
16	000000	C	Stack HOSTIP address
16	000010	C	Interface physical address
4	000020	N	Interface index
4	000024	N	Interface type
4	000028	N	Interface MTU
4	00002C	N	Interface speed
4	000030	N	Interface operator status
4	000034	N	Interface in octets
4	000038	N	Interface in unicast packets
4	00003C	N	Interface in non-unicast packets
4	000040	N	Interface in discards

Length	Offset (hex)	Type	Description
4	000044	N	Interface in errors
4	000048	N	Interface unknown protocols
4	00004C	N	Interface out octets
4	000050	N	Interface out unicast packets
4	000054	N	Interface out non-unicast packets
4	000058	N	Interface out discards
4	00005C	N	Interface out errors
4	000060	N	Interface out queue length
76	000064	C	Interface description

## Type I (TCP Connection) Entry

Type I records are TCP connection records, written each interval when TCP collection and logging is turned on. TCP=(Y,Y)

Fields are stack type specific. All fields are available for IBM type stacks unless indicated otherwise.

Length	Offset (hex)	Type	Description
16	000000	C	Connection local address (Stack type = I/O)
6	000010	C	Connection local port (Stack type = I/O)
16	000016	C	Connection remote address (Stack type = I/O)
6	000026	C	Connection remote port (Stack type = I/O)
8	00002C	C	Client name
8	000034	C	Server name (application name)
8	00003C	C	LU name
1	000044	N	TCP/IP protocol
7	000045		Reserved
4	00004C	N	Last touched
4	000050	N	Number of bytes sent
4	000054	N	Number of bytes received

Length	Offset (hex)	Type	Description
4	000058	N	Number of retransmitted bytes
4	00005C	N	Maximum send window
4	000060	N	Maximum send segment size
4	000064	N	Congestion window
4	000068	N	Slow start
4	00006C	N	Round trip time
4	000070	N	Round trip time variance
4	000074	N	Duplicate packs
4	000078	N	Optimal segment size
4	00007C	N	State - (stack type = 0)
4	000080	N	Out buffer
4	000084	N	In buffer
4	000088	N	Receive buffer size
8	00008C	C	Logmode
8	000094	C	VTAM Net ID (Telenet only)
8	00009C	C	VTAM User ID (Telenet only)
4	0000A4	N	VTAM number of transactions (Telenet only)
4	0000A8	N	VTAM number of outputs (Telenet only)
4	0000AC	N	VTAM average response HOST (Telenet only)
1	0000B0	N	Socket option
1	0000B1	N	Timer
1	0000B2	N	Signal

## Type J (Stack) Entry

Type J records are OS/390 and z/OS TCP/IP stack records, written each interval when STACK collection and logging is turned on. STACK=(Y,Y).

All fields are available for both Other and IBM type stacks unless indicated otherwise.

Length	Offset (hex)	Type	Description
4	000000	N	Receive buffer size (IBM stack type only)
4	000004	N	Send buffer size (IBM stack type only)
8	000008	N	TCP/IP IPL date and time (IBM stack type only)
4	000010	N	Maximum number of socket connections (MIIBII)
8	000014	C	TCP/IP procedure name
4	00001C	N	Minimum retransmission time
4	000020	N	Maximum retransmission time
4	000024	N	Limit on number of connections supported
4	000028	N	Active opens
4	00002C	N	Passive opens
4	000030	N	Number of failed connection attempts
4	000034	N	Number of resets
4	000038	N	Current established on closed-wait connections
4	00003C	N	Received segments
4	000040	N	Sent segments
4	000044	N	Retransmitted segments
4	000048	N	Segments with errors
4	00004C	N	Reserved
4	000050	N	TCP/IP address space ID
4	000054	N	UDP receiver buffer size
4	000058	N	UDP send buffer size
4	00005C	N	IF (interface) number
4	000060	N	IP forwarding
4	000064	N	IP in receives
4	000068	N	IP header errors
4	00006C	N	IP address errors
4	000070	N	IP forward datagrams
4	000074	N	IP unknown protocols
4	000078	N	IP input discards (for lack of buffer space)
4	00007C	N	IP input successfully delivered

Length	Offset (hex)	Type	Description
4	000080	N	IP output requests
4	000084	N	IP output discards
4	000088	N	IP out no routes
4	00008C	N	IP reassembly timeouts
4	000090	N	IP reassembly required
4	000094	N	IP reassembly OKs
4	000098	N	IP reassembly failures
4	00009C	N	IP fragmented OKs
4	0000A0	N	IP fragmented failures
4	0000A4	N	IP fragment creates
4	0000A8	N	IP valid routing entries discarded
4	0000AC	N	TCP segments sent containing RST flags
4	0000B0	N	UDP datagrams delivered to UDP customers
4	0000A4	N	UDP no ports
4	0000A8	N	UPD in errors
4	0000BC	N	UDP out datagrams

## Type M (MNPS Application) Entry

Type M entries for MNPS application records are described in the table below. These entries contain 32 bytes.

Length	Offset	Type	Description
8	0	C	Application program name
16	8	C	Coupling facility structure name
4	24	N	Number of coupling facility writes for this application
4	28	N	Number of bytes written to the coupling facility structure

## Generic Type N Entry

All type N entries (line, controller, terminal, NCP major node, NPSI, NTRI, TIC3, Ethernet Adapter, Frame Relay, and NCP control block information) fit into the format described below, which serves as an overview of all the possible flag values. Each of the specific N entries are described in their own section.

Length	Offset	Type	Description
8	0	C	Element name
4	8	N	NCP interval
1	12	N	Element type: <hr/> For Line, Controller, Terminal: X'49' - ESCON and CLA extended link X'29' - ESCON and CLA extended PU X'41' - Link X'40' - Line X'21' - PU X'20' - Cluster X'11' - LU X'10' - Terminal <hr/> For NCP: X'80' - NCP major node <hr/> For NPSI: X'49' - X.25 MCH line, XI line X'29' - X.25 MCH PU or X.25 VC, XI PU <hr/> For NTRI: X'71' - PLINKS (physical links) X'70' - LLINKS (logical links) <hr/> For Ethernet Adapter: X'49' - physical links <hr/> For Frame Relay: X'49' - physical and logical links X'29' - physical units <hr/> For TIC3: X'49' - physical links X'29' - physical units <hr/> For TP (Transmission Priority) X'49' - CLA extended link X'29' - CLA extended PU X'41' - Link X'21' - PU

Length	Offset	Type	Description
			For NCP control block information: X'89' - NCP control block information
			For HPR (High Performance Routing): X'71' - NTRI physical links X'70' - NTRI logical links X'49' - Frame Relay physical and logical links X'29' - Frame Relay physical units
58	13	N	Value
1	71	N	Resource subtype flag: For Line, Controller, Terminal: X'80' - Channel adapter X'40' - ACL line X'20' - Dial-up line X'00' - No value For NCP: X'00' - No value For NPSI: X'20' - Dial-up line X'04' - X.25 and XI extended resource For NTRI: X'08' - NTRI resource For Ethernet Adapter: X'01' - Ethernet resource For Frame Relay: X'02' - Frame Relay For TIC3: X'01' - TIC3 utilization X'00' - TIC3 base support For TP: X'80' - Channel adapter X'40' - ACL line X'20' - Dial-up line X'00' - No value For NCP Control Block Pool: X'00' - No value For HPR (High Performance Routing): X'08' - NTRI resource X'02' - Frame Relay resource
1	72	N	NCP Entry Extended Subtype:

Length	Offset	Type	Description
			For Line, Controller, Terminal: X'80' - ESCON X'40' - CLA
			For NCP major node: X'80' - Standard NCP major node
			For NPSI: X'80' - X.25 MCH line X'40' - X.25 MCH PU X'20' - X.25 VC X'10' - X.25 LU X'08' - X.25 XI X'04' - X.25 ODLC
			For NTRI: X'80' - Logical link X'40' - Physical link
			For Ethernet Adapter: X'80' - Physical link
			For Frame Relay: X'80' - Physical link X'40' - Logical link X'20' - Physical unit X'10' - LMI station X'08' - FRSE
			For TIC3: X'40' - physical link X'08' - physical unit
			For TP: X'80' - standard TP data X'40' - CLA TP data
			For NCP control block information: X'80' - standard NCP control block pool
			For HPR (High Performance Routing): X'80' - NTRI logical link or Frame Relay physical link X'40' - NTRI physical link or Frame Relay logical link X'20' - Frame Relay physical unit X'10' - LMI station X'08' - FRSE

Length	Offset	Type	Description
1	73	N	NCP record identifier X'0A' - HPR (High Performance Routing) data X'09' - NCP control block pool record X'08' - Transmission priority record X'07' - TIC3 resource X'06' - Ethernet adapter resource X'05' - Frame Relay resource X'04' - X.25 resource X'03' - NTRI resource X'02' - NCP major node record X'01' - Line, controller, terminal resource
32	74	N	Values

## Type N (HPR) Entry

Type N entries for High Performance Routing records are described in the table below. These entries contain 106 bytes.

Length	Offset	Type	Description
8	0	C	Element name
4	8	N	NCP collection interval (in tenths of seconds)
1	12	N	Element type: X'71' - NTRI physical link X'70' - NTRI logical link X'49' - Frame Relay physical or logical link X'29' - Frame Relay physical unit
4	13	N	Number of HPR frames sent
4	17	N	Number of HPR frames received
4	21	N	Number of HPR bytes sent
4	25	N	Number of HPR bytes received
4	29	N	Number of HPR bytes queued for transmission
4	33	N	Number of transmit HPR frames discarded for exceeding the transmit queue threshold
4	37	N	Number of received HPR frames discarded due to congestion in this node
30	41	C	Reserved

Length	Offset	Type	Description
1	71	N	Resource type: X'08' - NTRI resource X'02' - Frame Relay resource
1	72	N	Resource extended subtype: <i>NTRI resources only:</i> X'80' - Logical link X'40' - Physical link <i>Frame Relay resources only:</i> X'80' - Physical link X'40' - Logical link X'20' - Physical unit X'10' - LMI station X'08' - FRSE
1	73	N	NCP record identifier: X'0A' - HPR (High Performance Routing)
32	74	C	Reserved

## Type N (Line, Controller, Terminal) Entry

Type N entries for lines, controllers, and terminals are described in the table below. These entries contain 106 bytes and have information about the lines, controllers, and terminals within the NCPs that NetSpy is monitoring and that have an associated SMF record request specified through an SSMF command.

Length	Offset	Type	Description
8	0	C	Element name
4	8	N	NCP collection interval (in tenths of seconds)
1	12	N	Element type: X'49' - ESCON and CLA extended link X'29' - ESCON and CLA extended PU X'41' - Link X'40' - Line X'21' - PU X'20' - Cluster X'11' - LU X'10' - Terminal
4	13	N	Total messages sent

Length	Offset	Type	Description
4	17	N	Total messages received
4	21	N	Total bytes sent
4	25	N	Total bytes received
2	29	N	Outbound queue length
4	31	N	Total poll count
4	35	N	Positive poll count
2	39	N	Error count
4	41	N	Number of messages retransmitted
4	45	N	Number of bytes retransmitted
4	49	N	Line send speed
4	53	N	Line receive speed
2	57	N	Network address for element/element address if ENA
2	59	C	Element count for NCP entry
2	61	N	Pause, in tenths of seconds
2	63	N	REPLYTO
2	65	N	MAXDATA
1	67	N	MAXOUT
1	68	N	PASSLIM
1	69	N	PACING
1	70	N	SERVLIM
1	71	N	Resource subtype flags: X'80' - Channel adapter X'40' - ACL line X'20' - Dial-up line X'00' - No value
1	72	N	NCP entry extended subtype: X'80' - ESCON X'40' - CLA X'00' - No value
1	73	N	NCP record identifier: X'01' - Line, controller, terminal
8	74	N	VTAM switched definition PU name if available

**ESCON and CLA only:**

Length	Offset	Type	Description
4	82	N	NB channel count
4	86	N	Rate adapted
1	90	N	Status flag: X'80' - Resource was reset during interval
15	91	N	Reserved

## Type N (NCP Major Node) Entry

Type N (NCP major node) entries, described in the table below, contain 158 bytes and supply information about the NCP major nodes that NetSpy is monitoring and that have an associated SMF record request specified through an SSMF command.

Length	Offset	Type	Description
8	0	C	NCP name
4	8	N	NCP collection interval (in tenths of seconds)
1	12	N	Element type (X'80'- NCP)
4	13	N	Used cycle count
2	17	N	Current free buffer queue length
2	19	N	Free buffer high watermark
2	21	N	Free buffer low watermark
2	23	N	NCP channel intermediate queue length
2	25	N	NCP channel hold queue length
2	27	N	Time in slowdown (in tenths of seconds)
2	29	N	Number of free buffers at slowdown
2	31	N	Maximum free buffers
2	33	N	CCU cycle speed
4	35	N	Current free buffer queue length
4	39	N	Free buffer queue length high water mark
4	43	N	Free buffer queue length low water mark
4	47	N	Total free queue buffers allocated in the NCP

Length	Offset	Type	Description												
10	51	C	Reserved												
2	61	N	Delay value in tenths of seconds												
8	63	C	Reserved												
1	71	N	Resource Subtype Flag: X'00' - No value												
1	72	N	NCP Entry Extended Subtype: X'80' - Standard NCP major node												
1	73	N	NCP Record Identifier: X'02' - NCP major node												
<i>For NCP 7.2 and above:</i>															
4	74	N	Maximum number of buffers used by dynamic control blocks (DCBs)												
4	78	N	Maximum number of buffers available for use by DCBs												
4	82	N	Number of buffers currently in use												
<i>For NCP 7.3 and above:</i>															
72	86	N	CSS processor record, which contains 18 entries in the following format: <table border="0" style="margin-left: 40px;"> <tr> <td>0(0)</td> <td>1(1)</td> <td>2(2)</td> <td>3(3)</td> </tr> <tr> <td>RURRPTYP</td> <td>RURRUTIL</td> <td>RURRSDSU</td> <td>RURRPDSU</td> </tr> <tr> <td>CSS processor type</td> <td>CSS processor utilization</td> <td>CSS processor shared data store utilization</td> <td>CSS processor program data store utilization</td> </tr> </table>	0(0)	1(1)	2(2)	3(3)	RURRPTYP	RURRUTIL	RURRSDSU	RURRPDSU	CSS processor type	CSS processor utilization	CSS processor shared data store utilization	CSS processor program data store utilization
0(0)	1(1)	2(2)	3(3)												
RURRPTYP	RURRUTIL	RURRSDSU	RURRPDSU												
CSS processor type	CSS processor utilization	CSS processor shared data store utilization	CSS processor program data store utilization												

**Note:** For details on CSS processor types, refer to IBM's manuals on NCP.

## Type N (NPSI) Entry

Type N entries for X.25 NPSI records are described in the table below. These entries contain 106 bytes and supply information about X.25 multi-channel (MCH) lines, X.25 MCH PUs, X.25 virtual circuits, XI lines, and XI PUs.

Length	Offset	Type	Description
8	0	C	Element name
4	8	N	NCP collection interval in tenths of seconds
1	12	N	Element type: X'49' - X.25 MCH line, XI line X'29' - X.25 MCH PU or X.25 VC, XI PU
4	13	N	Total number of messages sent:

Length	Offset	Type	Description
			I-frames for X.25 MCH lines, XI lines, and XI PUs Packets for X.25 MCH PUs and X.25 VCs
4	17	N	Total number of messages received:  I-frames for X.25 MCH lines, XI lines, and XI PUs Packets for X.25 MCH PUs and X.25 VCs
4	21	N	Total number of bytes sent for X.25 MCH lines, X.25 VCs, XI lines, and XI PUs
4	25	N	Total number of bytes received for X.25 MCH lines, X.25 VCs, XI lines, and XI PUs
2	29	N	Outbound queue length for X.25 MCH lines, XI lines, and XI PUs
4	31	N	Total number of RNR frames sent for X.25 MCH lines, X.25 MCH PUs, XI lines, and XI PUs
4	35	N	Total number of RNR frames received for X.25 MCH lines, X.25 MCH PUs, XI lines, and XI PUs
2	39	N	Total errors for XI lines and XI PUs
4	41	N	Number of I-frames retransmitted for MCH lines, XI lines, and XI PUs
4	45	N	Number of bytes retransmitted for MCH lines, XI lines, and XI PUs
4	49	N	Line send speed
4	53	N	Line receive speed
2	57	N	Network address
2	59	N	Element count
10	61	N	NCP element data (see NCP line entry)
1	71	N	Resource subtype:  X'20' - Dial-up line X'04' - X.25 extended resource
1	72	N	Resource extended subtype for X.25 extended resources:  X'80' - X.25 MCH line X'40' - X.25 MCH PU X'20' - X.25 VC X'10' - X.25 LU X'08' - X.25 XI X'04' - X.25 ODLC
1	73	N	NCP record identifier:  X'04' - X.25 resource

Length	Offset	Type	Description
8	74	N	VTAM switched definition PU name if available
<i>X.25 MCH lines, XI lines, and XI PUs only:</i>			
4	82	N	Total number of RR frames sent
4	86	N	Total number of RR frames received
16	90	N	Reserved
<i>X.25 MCH PUs only:</i>			
2	82	N	Current number of VCs established
2	84	N	Number of new VCs established this interval
4	86	N	Total number of outbound connections (calls)
4	90	N	Total number of inbound connections (calls)
4	94	N	Total number of outbound disconnections (clears)
4	98	N	Total number of inbound disconnections (clears)
4	102	N	Total number of INN-SHM connections
<i>X.25 VCs only:</i>			
4	82	N	Total number of D-bit packets sent
4	86	N	Total number of D-bit packets received
4	90	N	Total number of M-bit packets sent
4	94	N	Total number of M-bit packets received
8	98	N	Reserved

## Type N (NTRI) Entry

Type N entries for NTRI records are described in the table below. These entries contain 106 bytes each for LLINK and PLINK resources.

Length	Offset	Type	Description
8	0	C	Element name
4	8	N	NCP collection interval in tenths of seconds
1	12	N	Element type: X'70' - logical link

Length	Offset	Type	Description
			X'71' - physical link
4	13	N	I-frames sent
4	17	N	I-frames received
4	21	N	Bytes sent
4	25	N	Bytes received
4	29	N	Outbound queue length
1	33	N	Reserved
1	34	N	Content flag 1
1	35	N	Content flag 4
1	36	N	Content flag 5
4	37	N	Total error count
4	41	N	Number of retransmitted I-frames
4	45	N	Number of retransmitted bytes
4	49	N	Transmit line speed
4	53	N	Receive line speed
2	57	N	NCP element address
2	59	N	Element count
4	61	N	Total frames sent
4	65	N	Total frames received
2	69	N	Reserved
1	71	N	Resource subtype: X'08' - NTRI resource
1	72	N	Resource extended subtype: X'80' - NTRI Logical Link X'40' - NTRI Physical Link
1	73	N	NCP record identifier: X'03' - NTRI resource
8	74	N	VTAM switched definition PU name if available
			<i>NTRI logical link - X'70' only:</i>
4	82	N	Reply time-outs
20	86	N	Reserved

Length	Offset	Type	Description
<i>NTRI physical link - X'71' only:</i>			
4	82	N	Active logical connections
4	86	N	Congestion count
4	90	N	Time per byte sent, in nanoseconds
4	94	N	Time per byte received, in nanoseconds
4	98	N	Time per frame sent, in microseconds
4	102	N	Time per frame received, in microseconds

## Type N (TIC3) Entry

Type N entries for TIC3 records are described in the table below. These entries contain 94 bytes for Physical Link resources and 94 bytes for Logical PU (LAN Stations) resources.

Length	Offset	Type	Description
8	0	C	Element name
4	8	N	NCP collection interval in tenths of seconds
1	12	N	Element type: X'49' - Physical link X'29' - Physical unit
4	13	N	I-frames sent
4	17	N	I-frames received
4	21	N	Bytes sent
4	25	N	Bytes received
2	29	N	Reserved
4	31	N	Total frames sent
4	35	N	Total frames received
2	39	N	Reserved
4	41	N	Retransmitted frames
4	45	N	Retransmitted bytes
4	49	N	Transmit line speed, if available

Length	Offset	Type	Description
4	53	N	Receive line speed, if available
2	57	N	NCP element address
2	59	N	NCP element count
4	61	N	Time per byte sent, in nanoseconds
4	65	N	Time per byte received, in nanoseconds
2	69	N	Reserved
1	71	N	Resource subtype: X'00' - TIC3 base support X'01' - TIC3 utilization
1	72	N	Resource extended subtype: X'40' - Physical link X'08' - Logical PU
1	73	N	NCP record type identifier: X'07' - TIC3 resource record
8	74	C	VTAM switched definition PU name, if available
<b>TIC3 Physical Link only (Extended Subtype X'40'):</b>			
4	82	N	Misaddressed frames received
4	86	N	Discarded frames
4	90	N	Unrecognized frames
4	94	N	Reserved
<b>TIC3 Logical PU only (Extended Subtype X'08'):</b>			
4	82	N	Local busy occurrences
4	86	N	Rejected frames sent
4	90	N	Rejected frames received
4	94	N	LAN T2 timeouts
<b>For TIC3LINKs and TIC3PUs:</b>			
4	98	N	Time per frame sent, in microseconds
4	102	N	Time per frame received, in microseconds

## Type N (Ethernet Adapter) Entry

Type N entries for Ethernet Adapter records are described in the table below. These entries contain 106 bytes.

Length	Offset	Type	Description
8	0	C	Element name
4	8	N	NCP collection interval in tenths of seconds
1	12	N	Element type: X'49' - Ethernet physical link
4	13	N	I-frames sent
4	17	N	I-frames received
4	21	N	Total bytes sent
4	25	N	Total bytes received.
2	29	N	Outbound queue length
4	31	N	Total frames sent
4	35	N	Total frames received
32	39	N	Reserved
1	71	N	Resource subtype: X'01' - Ethernet resource
1	72	N	Resource extended subtype: X'80' - Ethernet physical link
1	73	N	NCP record identifier: X'06' - Ethernet adapter
8	74	N	Reserved
4	82	N	Congestion count
4	86	N	Transmission deferred count
4	90	N	One collision count
4	94	N	Multiple collision count
4	98	N	Discarded datagrams
4	102	N	Reserved

## Type N (Frame Relay) Entry

Type N entries for Frame Relay records are described in the table below. These entries contain 106 bytes.

Length	Offset	Type	Description
8	0	C	Element name.
4	8	N	NCP collection interval in tenths of seconds.
1	12	N	Element type: X'49' - Frame Relay (physical links) X'49' - Frame Relay (logical links) X'29' - Frame Relay (physical units)
4	13	N	I-frames sent - PLINK and LLINK only.
4	17	N	I-frames received - PLINK and LLINK only
4	21	N	Total bytes sent.
4	25	N	Total bytes received.
2	29	N	I-frames on link outbound queue - PLINK, LLINK, and FRSE only
4	31	N	Total frames sent.
4	35	N	Total frames received.
2	39	N	Reserved
4	41	N	Number of I-frames retransmitted - PLINK and LLINK only
4	45	N	Number of bytes retransmitted - PLINK and LLINK only.
22	49	C	Reserved.
1	71	N	Resource subtype: X'02' - Frame Relay
1	72	N	Resource extended subtype: X'80' - Frame Relay (physical links) X'40' - Frame Relay (logical links) X'20' - Frame Relay (physical units) X'10' - Frame Relay (LMI stations) X'08' - Frame Relay (FRSE)
1	73	N	NCP record identifier: X'05' - Frame Relay
8	74	C	Reserved

Length	Offset	Type	Description
<i>Frame Relay Entry - (physical link section) only:</i>			
X'49' - Frame Relay physical link Offset 12			
X'80' - Frame Relay physical link Offset 72			
2	82	N	Number of active logical connections
4	84	N	Number of frames with forward congestion.
4	88	N	Number of frames with backward congestion.
4	92	N	Number of frames discarded.
10	96	N	Reserved.
<i>Frame Relay Entry - (logical link section) only:</i>			
X'49' - Frame Relay logical link Offset 12			
X'40' - Frame Relay logical link Offset 72			
4	82	N	Number of reply timeouts
4	86	N	Number of frames with forward congestion.
4	90	N	Number of frames with backward congestion.
12	94	N	Reserved.
<i>Frame Relay Entry - (LMI station section) only:</i>			
X'29' - Frame Relay PU Offset 12			
X'20' - Frame Relay physical unit Offset 72			
X'10' - Frame Relay LMI station Offset 72			
4	82	N	Number of frames discarded.
20	86	N	Reserved.
<i>Frame Relay Entry - (FRSE station section) only:</i>			
X'29' - Frame Relay PU Offset 12			
X'20' - Frame Relay physical unit Offset 72			
X'08' - Frame Relay FRSE Offset 72			
4	82	N	Number of frames with forward congestion.
4	86	N	Number of frames with backward congestion.
4	90	N	Number of frames discarded.
12	94	N	Reserved.

## Type N (NCP Control Block Information) Entry

Type N entries for NCP control block information are described in the table below. These entries contain 158 bytes.

Length	Offset	Type	Description
8	0	C	Network ID
4	8	N	NCP collection interval in seconds
1	12	N	Element type: X'89' - NCP control block information
2	13	N	Control block pool/table identifier: X'0000' - Buffer pool, 1 per NCP, no associated generation parameter X'0001' - BSB pool (independent LUs), 1 per NCP, ADDSESS on BUILD X'0002' - CUB pool (PU DR pool), 1 per NCP, NUMBER on PUDRPOOL X'0003' - FCT (flow control parameter table), 1 per NCP, VRPOOL on BUILD X'0004' - Token ring LLB pool, 1 per NCP, AUTOGEN on GROUP X'0006' - LND/LNB pool (dependent LUs), 1 per NCP, NUMTYP1/NUMTYP2 on LUDRPOOL X'0007' - LTX pool, 1 per NCP, NUMTYP1 on LUDRPOOL X'0008' - LUB pool (LU DR pool), 1 per NCP, NUMILU/NUMTYP1/NUMTYP2 on LUDRPOOL X'0009' - LUX pool, 1 per NCP, BACKUP on BUILD X'000A' - SNI NLD/NIB pair pool (GWNAUS), 1 per NCP, NUMADDR on GWNAU X'000B' - NIX/NLX pair pool (HSB pool), 1 per NCP, HSBPOOL on BUILD X'000C' - NNT (network names table), 1 per NCP, NAMTAB on BUILD X'000D' - NQE pool, 1 per NCP, MAXCOLL on NPA LU X'000E' - NQX pool, 1 per NCP, MAXTP on NPA LU X'000F' - NSB pool, 1 per NCP, FRSEDRPU on PUDRPOOL X'0010' - NSC pool, 1 per NCP, GWSESAC/SESSACC on BUILD X'0011' - NSX pool, 1 per NCP, GSWEWESAC/SESSACC on BUILD X'0012' - NVT (network vector table), 1 per NCP, copies on network X'0013' - ODLC LAN logical resources pool, 1 per NCP, AUTOGEN on

Length	Offset	Type	Description
			ONGROUP
			X'0014' - Free RVT entry pool, 1 per NCP, no associated generation parameter
			X'0015' - TGB pool, 1 per network, TGBXTRA on BUILD and NETWORK
			X'0015' - TGB pool, 1 per network, TGBXTRA on BUILD and NETWORK
			X'0016' - TRT (transit routing table), 1 per network, PATHEXT on BUILD and NETWORK
			X'0017' - VST and VAT (virtual route status table and virtual route access table), 1 per NCP, NUMHSAS on BUILD and NETWORK
			X'0018' - VTS (vector table of SNP, SNP pool), 1 per NCP, MAXSSCP on BUILD
			X'0019' - VVT (VR vector table, VRB pool), 1 per NCP, VRPOOL on BUILD
			X'001A' - Frame relay LLB pool, 1 per NCP, AUTOGEN on GROUP
			X'0028' - HRE pool, 1 per NCP, NUMROUTE on IPOWNER
			X'0029' - SRE pool, 1 per NCP, NUMROUTE on IPOWNER
			X'002A' - NRE pool, 1 per NCP, NUMROUTE on IPOWNER
1	15	N	Control block flag: X'80' - Pool/table supports dynamic creation of control blocks
3	16	N	Reserved
4	19	N	Pool size: initial size of pool obtained from the number of in-use and free control blocks after NCP initialization. Permanently assigned control blocks are not included.
4	23	N	Initial number of in-use control blocks/entries
4	27	N	Initial number of free control blocks/entries
4	31	N	Maximum number of in-use control blocks/entries since NCP was last initiated. Buffer pool value is only approximate.
4	35	N	Number of buffers from the buffer pool currently being used for this type of control block. For the buffer pool, it's the total number of buffers currently being used for control blocks and table entries.
4	39	N	Maximum number of in-use control blocks/entries during the interval. Buffer pool value is only approximate.
4	43	N	Number of control blocks/entries currently in use.

Length	Offset	Type	Description
4	47	N	Minimum number of in-use control blocks/entries during the interval. Buffer pool value is only approximate.
4	51	N	Maximum number of free control blocks/entries in the unreserved pool/table during the interval. Buffer pool value is only approximate.
4	55	N	Number of free control blocks/entries currently in the the unreserved pool/table.
4	59	N	Minimum number of free control blocks/entries in the unreserved pool/table during the interval. Buffer pool value is only approximate.
4	63	N	Maximum number of free control block/entries in reserved pool/table during the interval.
4	67	N	Number of free control block/entries currently in the reserved pool/table.
1	71	N	Resource subtype: X'00' - no value
1	72	N	NCP entry extended subtype: X'80' - standard NCP control blocks
1	73	N	Resource subtype: X'09' - NCP control block pool
4	74	N	Minimum number of free control blocks/entries in the reserved pool/table during the interval.
4	78	N	Maximum number of control blocks/entries from buffer pool during the interval. For buffer pool, maximum number of buffers being used for control blocks and table entries during the interval.
4	82	N	Number of in-use control blocks/entries currently from the buffer pool. For buffer pool, total number of buffers currently used for control blocks (same as the value at offset 35).
4	86	N	Minimum number of control blocks/entries from buffer pool during the interval. For buffer pool, minimum number of buffers being used for control blocks and table entries during the interval.
4	90	N	Number of permanently assigned control blocks/entries from system generation.
64	94	N	Reserved.

## Type N (Transmission Priority) Entry

Type N entries for transmission priority records are described in the table below. These entries contain 106 bytes.

Length	Offset	Type	Description
8	0	C	Name
4	8	N	NCP interval
1	12	N	Element type: X'49' - CLA extended link X'29' - CLA extended PU X'41' - link X'21' - PU
4	13	N	Number of high priority I-frames sent
4	17	N	Number of high priority I-frames received
4	21	N	Number of high priority bytes sent
4	25	N	Number of high priority bytes received
4	29	N	Number of medium priority I-frames sent
4	33	N	Number of medium priority I-frames received
4	37	N	Number of medium priority bytes sent
4	41	N	Number of medium priority bytes received
4	45	N	Number of low priority I-frames sent
4	49	N	Number of low priority I-frames received
4	53	N	Number of low priority bytes sent
4	57	N	Number of low priority bytes received
10	61	N	Reserved
1	71	N	Resource subtype: X'80' - Channel adapter X'40' - ACL line X'20' - Dial-up line X'00' - No value
1	72	N	Resource extended subtype: X'80' - Standard TP X'40' - CLA TP
1	73	N	NCP record identifier: X'08' - TP (Transmission Priority)
32	74	N	Reserved

## Type P (APPN Topology) Entry

Type P entries for APPN Topology records are described in the table below. These entries contain 88 bytes.

Length	Offset	Type	Description
4	0	N	Number of routes calculated using an existing tree
4	4	N	Number of routes calculated using a modified tree
4	8	N	Number of routes calculated using a new tree
4	12	N	Number of topology database updates (TDUs) originated by this node
4	16	N	Number of TDUs propagated by this node
4	20	N	Number of TDUs received by this node resulting in a topology database update
4	24	N	Number of TDUs received by this node and discarded by this node for normal reasons. Resource sequence number (RSN) is valid, but data already seen
4	28	N	Number of TDUs received by this node and discarded because the RSN is not valid. (TDU is rebroadcast)
4	32	N	Number of TDUs received by this node and discarded because of data inconsistency. (TDU is rebroadcast)
4	36	N	Number of network nodes in the topology database
4	40	N	Number of end nodes in the topology database
4	44	N	Number of unidirectional TGs in the topology database
4	48	N	Number of TG failures at this node
4	52	N	Number of dynamic PU allocations
4	56	N	Number of times a routing tree was discarded due to the tree cache becoming full
4	60	N	Current number of trees in the tree cache
4	64	N	Number of virtual nodes in the topology database
4	68	N	Number of central directory server nodes in the topology database
4	72	N	Number of interchange nodes in the topology database
4	76	N	Number of end nodes connected to this node
4	80	N	Number of network nodes connected to this node
4	84	N	Number of virtual nodes connected to this node

## Type R (VTAM RTP) Entry

Type R entries for APPN RTP records are described in the table below. These entries contain 77 bytes.

Length	Offset	Type	Description
8	0	C	RTP physical unit
8	8	C	Remote network ID
8	16	C	Remote CP name
1	24	N	RTP state X'80' - ACTIVE X'40' - INACTIVE X'20' - NORMAL
4	25	N	Round trip delay
4	29	N	Number of bytes sent over the RTP
4	33	N	Number of bytes received over the RTP
4	37	N	Number of PIUs that were segmented sent over the RTP
4	41	N	Number of PIUs that were not segmented sent over the RTP
4	45	N	Number of PIUs that were segmented received over the RTP
4	49	N	Number of PIUs that were not segmented received over the RTP
2	53	N	Number of HPR path switch attempt initiated by other RTP endpoint
2	55	N	Number of HPR path switch attempts due to operator or VTAM command
2	57	N	Number of HPR path switch attempts due to any other failure (such as link failure or node failure)
2	59	N	Number of HPR path switch attempts due to operator or VTAM command that were unsuccessful
2	61	N	Number of HPR path switch attempts due to any other failure (such as link failure or node failure) that were unsuccessful
4	63	N	Number of active LU-LU sessions using the RTP
2	67	N	Number of times that back pressure has been applied due to HPR path switch
2	69	N	Number of time back pressure has been applied queue depth exceeded
2	71	N	Number of times back pressure applied due to storage shortage
4	73	N	Number of retransmitted NLPs

## Type S (Terminal Session) Entry

Type S (terminal session) entries, described in the following below, contain 164 bytes and supply information about session partners when a session is initiated or terminated. These records are written at session initiation or termination, rather than at the end of the base interval.

Initialization records contain the initiation time; termination records contain data from the beginning of the interval or the session's initiation, whichever is later.

You can collect type S and T records for the same terminal in the same interval: a type S record will be generated at session initiation, then at the end of the current interval, a type T record will be generated.

**Note:** The collection of type S records is optional. Records will be recorded unless you specify SESSION=NO in the SMF statement of the INITPRM member. *Type S records are never written to the Log or Database.*

Length	Offset	Type	Description
8	0	C	Terminal name (if a virtual terminal session, the virtual terminal name will always appear)
4	8	N	Terminal CID (network address)
4	12	C	Session type: <ul style="list-style-type: none"> <li>■ If initiation, INIT (with rest of record blank)</li> <li>■ If termination, END</li> </ul>
4	16	C	Reserved
4	20	N	Last host response time (in 2 <sup>16</sup> microseconds)
4	24	N	Last network response time (in 2 <sup>16</sup> microseconds)
4	28	N	Worst host response time (in 2 <sup>16</sup> microseconds)
4	32	N	Worst network response time (in 2 <sup>16</sup> microseconds)
4	36	N	Cumulative host response time (in 2 <sup>16</sup> microseconds)
4	40	N	Cumulative network response time (in 2 <sup>16</sup> microseconds)
2	44	N	Number of inputs (initiated transactions)
2	46	N	Number of outputs
2	48	N	Number of network responses computed
2	50	N	Number of responses on target 1
4	52	N	Cumulative input length

Length	Offset	Type	Description
4	56	N	Cumulative output length
2	60	N	Number of responses on target 2
2	62	N	Number of responses on target 3
2	64	N	Number of responses on target 4
1	66	C	Reserved
1	67	N	Flag (X'04' - add 1 to the number of inputs to get the number of completed transactions at the host)
1	68	N	Flag (X'04' - represents a virtual session between a session manager and an application).
1	69	N	4 high order bits are virtual route
1	70	N	Reserved
1	71	N	Flag: <ul style="list-style-type: none"> <li>■ If X'01' bit, LU 6.2 traffic was detected on this session</li> <li>■ If X'02' bit, response times are not being collected for this session (see Note below for additional information)</li> <li>■ If X'04' bit, LU 6.2 response times for this session are measured with allocates and deallocates</li> <li>■ If X'80' bit, the session is between a terminal and the session manager</li> </ul>
16	72	C	Reserved
8	88	N	User ID for session LU. (See Note below.)
2	96	N	Global NTARGETs/UTARGETs #1 (number of responses on target)
2	98	N	Global NTARGETs/UTARGETs #2 (number of responses on target)
2	100	N	Global NTARGETs/UTARGETs #3 (number of responses on target)
2	102	N	Global NTARGETs/UTARGETs #4 (number of responses on target)
2	104	N	Reserved
2	106	N	Number of transactions terminated at the host
2	108	N	Number of transactions (Attaches) initiated on the LU 6.2 session
2	110	N	Number of user responses (for both LU 6.2 and non-LU 6.2)
8	112	N	Network ID of session LU (ESA only)
8	120	N	Procedure correlation ID (ESA only)
8	128	N	Virtual LU name (ESA only)
28	136	N	Reserved

Length	Offset	Type	Description
--------	--------	------	-------------

**Notes:** (1) The 'X02' bit added to the flag at decimal offset 71 indicates that response times are not being collected for this session. This means that the last host response, last network response, worst host response, worst network response, cumulative host response, cumulative network response, number of network responses computed, number of responses on targets, and number of transactions terminated at the host fields should not be used for summarizing or reporting information. These fields may contain data; however, this data should not be used for reporting. (2) For non-ESA releases, this field contains the TSO user ID. For ESA releases, this field can contain either the TSO user ID (for TSO sessions) or the CA-TPX user ID (for virtual non-TSO sessions).

## Type T and U (Terminal) Entries

Type T and U (terminal) entries, described in the table below, contain 164 bytes. Type T entries supply information about the terminals in session with an application that NetSpy was monitoring. NetSpy starts collecting this data at the beginning of the interval or when the terminal session is initiated, whichever is later.

Type U entries supply information about the terminals that ended sessions in the middle of an interval. NetSpy starts collecting this data at the beginning of the interval or when the terminal session is initiated, whichever is later, and continues to collect it until the session ends. NetSpy writes data to type U entries at the end of each base interval.

**Note:** Type U entries are optional for SMF recording. To collect them, you must specify TYPEU=YES on the SMF statement in the INITPRM member of the startup JCL. *Type U records are always written to a log file.*

Length	Offset	Type	Description
8	0	C	Terminal name
4	8	N	Terminal CID (network address)
8	12	C	Reserved for T records For U records only: Length 4, offset 12, type N: Session stop time Length 4, offset 16, type N: Session stop date
4	20	N	Last host response time (in 2 <sup>16</sup> microseconds)
4	24	N	Last network response time, calculated average network response time, or bid-to-poll delay; based on the flag at offset 71 (in 2 <sup>16</sup> microseconds)
4	28	N	Worst host response time (in 2 <sup>16</sup> microseconds)

Length	Offset	Type	Description
4	32	N	Worst network response time (in 2 <sup>16</sup> microseconds)
4	36	N	Cumulative host response time host (in 2 <sup>16</sup> microseconds)
4	40	N	Cumulative network response time (in 2 <sup>16</sup> microseconds)
2	44	N	Number of inputs (initiated transactions)
2	46	N	Number of outputs
2	48	N	Number of network responses computed
2	50	N	Number of responses on target 1
4	52	N	Cumulative input length
4	56	N	Cumulative output length
2	60	N	Number of responses on target 2
2	62	N	Number of responses on target 3
2	64	N	Number of responses on target 4
1	66	C	Reserved
1	67	N	Flag (X'04' bit - add 1 to the number of inputs to get the number of completed transactions at the host)
1	68	N	Flag (X'04' bit - represents a virtual session between a session manager and an application)
1	69	N	4 high order bits are virtual route
1	70	N	Reserved
1	71	N	Flag: <ul style="list-style-type: none"> <li>■ If X'04' bit, Telnet connection</li> <li>■ If X'10' bit, the field at offset 24 contains a calculated average network response time</li> <li>■ If X'20' bit, the field at offset 24 contains the average bid-to-poll delay for a transaction</li> <li>■ If X'40' bit, subtract 1 from the number of inputs to get the number of completed transactions at the host</li> <li>■ If X'80' bit, the session is between a terminal and the session manager</li> </ul>
8	72	C	Line name for this LU
8	80	C	Cluster controller name for this LU
8	88	C	User ID for session LU (See Note below.)
2	96	N	Global NTARGETs/UTARGETs #1 (number of responses on target)

Length	Offset	Type	Description
2	98	N	Global NTARGETs/UTARGETs #2 (number of responses on target)
2	100	N	Global NTARGETs/UTARGETs #3 (number of responses on target)
2	102	N	Global NTARGETs/UTARGETs #4 (number of responses on target)
2	104	N	Reserved
2	106	N	Number of transactions terminated at the host
2	108	N	Number of transactions (Attaches) initiated (for LU 6.2 sessions only)
2	110	N	Number of user responses (for both LU 6.2 and non-LU 6.2)
8	112	N	Network ID of session LU (ESA only)
8	120	N	Procedure correlation ID (ESA only)
8	128	N	Virtual LU name (ESA only)
28	136	N	Reserved

**Note:** For non-ESA releases, this field contains the TSO user ID. For ESA releases, this field can contain either the TSO user ID (for TSO sessions) or the CA-TPX user ID (for virtual non-TSO sessions).

## Type V (Virtual Route) Entry

Type V (virtual route) entries, described in the table below, contain 68 bytes and supply information about the virtual routes that NetSpy was monitoring at the end of the interval.

Length	Offset	Type	Description
2	0	N	Destination subarea
1	2	N	The VR ID (the first 4 bits) and the transmission priority (last 4 bits)
1	3	N	Status indicator: <ul style="list-style-type: none"> <li>■ X'0' - the virtual route is blocked</li> <li>■ X'01' - the virtual route is held</li> <li>■ X'03' - the virtual route is open</li> <li>■ X'FF' - the virtual route is inactive</li> </ul>
4	4	N	Total outbound PIUs
4	8	N	Measured outbound PIUs
4	12	N	Measured number of responses

---

<b>Length</b>	<b>Offset</b>	<b>Type</b>	<b>Description</b>
4	16	N	Cumulative network responses (in $2^{16}$ microseconds)
8	20	N	Cumulative output length
4	28	N	Cumulative time VR is held/blocked (in $2^{16}$ microseconds)
2	32	N	Residual pacing count
2	34	C	Reserved
4	36	N	Time of last pacing request
2	40	N	Number of LU-LU sessions on VR
2	42	N	Number of PIUs blocked or held
4	44	N	Time VR became blocked
4	48	N	Measured pacing requests (measured windows)
1	52	N	Minimum window size observed
1	53	N	Maximum window size observed
1	54	N	Reserved
1	55	N	Current window size at interval
4	56	N	Total number of inbound PIUs
8	60	N	Cumulative input length in bytes of inbound PIUs

---

## Type X (General Alert) Entry

Type X (general alert) entries, described in the table below, contains 94 to 204 bytes and supply information about the general alerts that NetSpy generates. When NetSpy writes these records depends on how you specified the ALWRITE parameter in the INITPRM member or file: either at the end of the interval when the general alerts occur, or when the logging I/O buffer is full.

**Note:** There is an 84-byte header + 10 bytes for each threshold exceeded. For LU monitors, there are 30 additional bytes for the FORAPPL, FORLINE, and FORPU selection parameters.

Length	Offset	Type	Description
8	0	N	Time alert was recorded
8	8	C	Name of monitor recording alert
8	16	C	NSYXNAME (name of cross-domain NetSpy which issued the alert)
8	24	C	Resource name
48	32	C	User-specified description of alert
1	80	N	Resource type: <ul style="list-style-type: none"> <li>■ X'00' - application program</li> <li>■ X'04' - NCP</li> <li>■ X'08' - line</li> <li>■ X'0C' - cluster</li> <li>■ X'10' - LU (see "variable type" in next section)</li> <li>■ X'14' - virtual route</li> <li>■ X'40' - TIC3 physical link</li> <li>■ X'41' - TIC3 logical PU</li> <li>■ X'42' - NTRI logical link</li> <li>■ X'43' - NTRI physical link</li> <li>■ X'44' - X.25 MCH line</li> <li>■ X'45' - X.25 MCH PU</li> <li>■ X'46' - X.25 virtual circuit</li> <li>■ X'47' - Frame Relay physical link</li> <li>■ X'48' - Frame Relay logical link</li> <li>■ X'49' - Frame Relay PU</li> <li>■ X'4A' - Ethernet physical link</li> </ul>

Length	Offset	Type	Description
1	81	N	<ul style="list-style-type: none"> <li>■ Routing destination flags:</li> <li>■ X'01' - Database</li> <li>■ X'02' - AccuMaster</li> <li>■ X'04' - NetView</li> <li>■ X'08' - SMF</li> <li>■ X'10' - Log</li> <li>■ X'20' - console</li> <li>■ X'40' - local</li> <li>■ X'80' - global</li> <li>■ X'FF' - all of the above</li> </ul>
2	82	N	Number of variable-value pairs in this record

**Note:** Up to and including the above, the type X record length is fixed. The variable length can be determined by multiplying the number of variable value pairs by the length of the variable value pair entry (in the following row).

10	84	N	Variable-value pair
1		N	Variable type: <ul style="list-style-type: none"> <li>■ X'00' - average host response time</li> <li>■ X'04' - average network response time</li> <li>■ X'08' - average user response time</li> <li>■ X'0C' - worst host response time</li> <li>■ X'10' - worst network response time</li> <li>■ X'14' - byte rate per second</li> <li>■ X'18' - transaction rate per minute</li> <li>■ X'1C' - NCP cycle utilization</li> <li>■ X'20' - NCP buffer utilization</li> <li>■ X'24' - NCP channel hold queue length</li> <li>■ X'28' - message rate per minute</li> <li>■ X'2C' - PIU segment rate per minute</li> <li>■ X'30' - error count</li> <li>■ X'34' - output queue length</li> <li>■ X'38' - utilization</li> <li>■ X'3C' - number of sessions</li> <li>■ X'40' - virtual route blocked/held</li> <li>■ X'44' - FORAPPL (if resource type is LU)</li> <li>■ X'4C' - FORLINE (if resource type is LU)</li> <li>■ X'50' - FORCLUSTER (if resource type is LU)</li> </ul>

Length	Offset	Type	Description
			Line and PU Resources:
			<ul style="list-style-type: none"> <li>■ X'A0' - retransmit messages</li> <li>■ X'A1' - retransmit bytes</li> </ul>
			NTRI Resources:
			<ul style="list-style-type: none"> <li>■ X'A0' - TIC utilization</li> <li>■ X'A1' - Iframes/minute</li> <li>■ X'A2' - bytes/second</li> <li>■ X'A3' - outbound queue length</li> <li>■ X'A4' - retransmit frames</li> <li>■ X'A5' - retransmit bytes</li> <li>■ X'A6' - congestion count</li> <li>■ X'A7' - active connections</li> <li>■ X'A8' - timeouts</li> </ul>
			X.25 Resources:
			<ul style="list-style-type: none"> <li>■ X'A0' - line utilization</li> <li>■ X'A1' - Iframes/minute</li> <li>■ X'A2' - outbound queue length</li> <li>■ X'A3' - packets/minute</li> </ul>
			Frame Relay Resources:
			<ul style="list-style-type: none"> <li>■ X'A0' - Iframes/minute</li> <li>■ X'A1' - bytes/second</li> <li>■ X'A2' - retransmit frames</li> <li>■ X'A3' - retransmit bytes</li> <li>■ X'A4' - outbound queue length</li> <li>■ X'A5' - discarded frames</li> <li>■ X'A6' - forward congestion</li> <li>■ X'A7' - backward congestion</li> </ul>

Length	Offset	Type	Description
			Ethernet Resources: <ul style="list-style-type: none"> <li>■ X'A0' - Iframes/minute</li> <li>■ X'A1' - bytes/second</li> <li>■ X'A2' - outbound queue length</li> <li>■ X'A3' - congestion count</li> <li>■ X'A4' - transmission deferred</li> <li>■ X'A5' - one collision</li> <li>■ X'A6' - multiple collisions</li> <li>■ X'A7' - discarded IP frames</li> </ul>
			TIC3 Resources: <ul style="list-style-type: none"> <li>■ X'A0' - Iframes/minute</li> <li>■ X'A1' - bytes/second</li> <li>■ X'A2' - retransmit Iframes</li> <li>■ X'A3' - retransmit bytes</li> <li>■ X'A4' - timeouts</li> <li>■ X'A5' - rejected frames</li> <li>■ X'A6' - discarded frames</li> </ul>
1		N	Operator type <ul style="list-style-type: none"> <li>■ X'80' - =</li> <li>■ X'40' - &lt;</li> <li>■ X'20' - &gt;</li> <li>■ X'D0' - &lt;=</li> </ul>
4		N	User-specified threshold
4		N	Current reported value

**Note:** If resource type is LU, the first three variable value pairs are types 44, 4C and 50. These represent the application, line, and cluster for the LU. In each case, the user-specified threshold and current reported value will show an eight-byte application, line, or cluster name.

## Trace Record Layout

Exception and transaction-all trace records, described in the table below, contain the output generated by NetSpy's exception trace facility.

Length	Offset	Type	Description
<b>Trace Record Header</b>			
4	0	N	RDW for buffer
4	4	C	Trace record ID ("NSYT")
4	8	N	Date first PIU in transaction was traced (in packed decimal form 00yydddf)
4	12	N	Time first PIU in transaction was traced (hundredths of seconds since midnight)
4	16	N	Number of transactions in buffer
12	20	N	Reserved
<b>Transaction Header</b>			
4	0	N	Entry length of transaction
8	4	C	Application name being traced
8	12	C	LU name being traced
2	20	N	Transaction host response time (in $2^{16}$ microseconds)
2	22	N	Transaction network response time (in $2^{16}$ microseconds)
1	24	N	Flag for this transaction (X'80' - virtual LU being traced)
<b>PIU Entry</b>			
2	0	N	Length for this PIU entry
1	2	N	Flag for this PIU: <ul style="list-style-type: none"> <li>■ X'80' - inbound flow</li> <li>■ X'40' - not first PIU segment (no RH)</li> </ul>
5	3	N	Date and time of PIU (5 high-order bytes of CPU clock)
2	8	N	Number of bytes in PIU (RH + RU)
3	10		RH being traced
Length of RU (length for this PIU entry minus 13)	13		RU

Length	Offset	Type	Description
<b>Buffer Trace Record Layout, Block Level Data</b>			
4	0	N	Block descriptor word
<b>Buffer Trace Record Layout, Record Level Data</b>			
2	0	N	Record length
4	2		Reserved
8	6	N	Time record was written
2	14	N	VTAM log ID (X'E019')
4	16	N	ASCB pointer for writing job
8	20	C	Job name of task
2	28	N	ID of record
8	30	N	Time of day
1	38	N	Buffer type (1=in, 2=out)
1	39	N	Flag for this PIU: X'03' - only record in PIU
8	40	C	Destination LU name
4	48	N	Destination subarea
2	52	N	Destination element address
8	54	C	Origin LU name
4	62	N	Origin subarea
2	66	N	Origin element address
26	68	X	Transmission header (TH)
3	94	X	Request/response header (RH)
	97	X	Start of RU data

# Converting NCP Records to Type 38 Format

NetSpy provides an NCP interface that collects NCP data and writes it in NetSpy subtype N records (the user specifies the SMF type). These records later serve as input for the NetSpy batch reports or online historical displays. The NetView Performance Monitor (NPM) also collects and logs this data in an SMF type 38 record.

## Using the NSYCONV Conversion Utility

Although NetSpy includes its own reporting programs, you may already have existing programs that process type 38 records. NSYCONV is a NetSpy utility that converts NetSpy subtype N records to NPM type 38 records. This utility allows you to continue to use your programs that only accept NPM type 38 format records.

The NSYCONV program accepts parameter statements to specify input and control parameters. See [NSYCONV Program Statements](#) in this chapter for an explanation.

The complete JCL for executing NSYCONV on an OS/390 and z/OS system is shown below. Member NSYCONV of *dsnpref.NYvvv.CNTL* contains sample JCL for executing NSYCONV.

```
//MYJOB JOB etc.           ...your JOB card
//STEP1 EXEC PGM=NSYCONV  ...the EXEC card
//STEPLIB DD DSN=etc.     ...the LOADLIB containing NSYCONV
//SYSPRINT DD SYSOUT=A   ...for output messages
//SYSUT1  DD DSN=etc.    ...input data set with the NetSpy records
//SYSUT2  DD DSN=etc.,  ...output data set for the type 38 records
// DCB=(DSORG=PS,LRECL=32756,
//      BLKSIZE=4096,RECFM=VBS)
//SYSIN   DD *
...           ...the NSYCONV parameter statements
/*
//
```

## NSYCONV Program Statements

The following statements are allowed with NSYCONV. These include a date and time range and the record type. The input and output records also can be printed using a DUMP parameter.

### Start and Stop Time Parameters

These statements specify a start and stop date, time, or both. The formats are:

```
START TIME=time
START DATE=date
START DATE=date, TIME=time
STOP TIME=time
STOP DATE=date
STOP DATE=date, TIME=time
```

---

<b>Date/time Values:</b>	<b>Explanation</b>
--------------------------	--------------------

---

<i>hh:mm:ss</i>	Indicates hours:minutes:seconds.
-----------------	----------------------------------

---

<i>mm/dd/yy</i>	Indicates month/day/year.
-----------------	---------------------------

---

Examples:

```
START DATE=01/02/95
START DATE=03/15/95, TIME=08:00:00
STOP DATE=01/12/95
STOP DATE=03/15/95, TIME=16:00:00
```

### Record Type Parameter

This statement specifies the NetSpy SMF record type to be converted. The format is:

```
SMFTYPE=n
```

---

<b>Operand</b>	<b>Explanation</b>
----------------	--------------------

---

SMFTYPE= <i>n</i>	Indicates the record number specified in the NetSpy installation using the statement SMF= <i>n</i> (OS/390 and z/OS only) or LOG= <i>n</i> .
-------------------	--

---

Examples:

```
SMFTYPE 132
SMFTYPE 128
```

## Print Parameter

This statement specifies which records are to be printed: either the original records or the converted records. The format is:

DUMP *record*

Operand	Explanation
<i>record</i>	Indicates the type of record that should be printed. Can have one of the following values:
INPUT	Original NetSpy records
OUTPUT	Type 38 records

Examples:

DUMP INPUT  
DUMP OUTPUT



# Converting Log Records to Type 28 Format

Although NetSpy includes its own reporting programs, you may already have existing programs that process type 28 records. Ideally, you should customize those programs to handle Log records. If that is not possible, you can use the N28CONV program to convert Log data into NPM type 28 record format.

## Using the N28CONV Conversion Utility

The log data input should be dumped from live SMF data sets to a sequential file on disk or tape. You can use the SMFDUMP job to do this.

**Note:** The SMF or log data used as input to N28CONV must have been collected by NetSpy Release 4.0 or higher.

The N28CONV program accepts parameter statements to specify input and control parameters. See [N28CONV Program Statements](#) in this chapter.

### N28CONV Utility

To run the N28CONV program on OS/390 and z/OS, edit and submit the JCL in the N28CONV member of the *dsnpref.NYvvv.CNTL* data set, shown below. The LRECL size specified for the SYSUT2 DD must be the same or larger than the LRECL specified for SYSUT1.

```
//N28CONV JOB 1,NS-N28CONV,CLASS=A,MSGCLASS=H,
//*****
//* THIS JOB CONVERTS NETSPY TYPE N RECORDS TO SMF TYPE 28
//*****
//N28CONV EXEC PGM=N28CONV
//STEPLIB DD DISP=SHR,DSN=dsnpref.NYvvv.NYLOAD <==* MOD
//SYSPRINT DD SYSOUT=*
//SNAPDCB DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//SYSUT1 DD DISP=SHR,DSN=dsnpref.NYvvv.LOGDUMP <==* MOD
//SYSUT2 DD DISP=(NEW,CATLG,DELETE),
// UNIT=SYSDA,DSN=USER.TYPE28, <==* MOD
// SPACE=(TRK,(50,10),RLSE), <==* MOD
// DCB=(DSORG=PS,LRECL=32756,BLKSIZE=4096,RECFM=VB)
//SYSIN DD *
START DATE=01/01/2000,TIME=00:00:00
STOP DATE=12/31/2000,TIME=24:00:00
SMFTYPE 132
ERROR MAX=5,PRINT=300
/*
//
```

## N28CONV Program Statements

You specify the statements below in the JCL.

### Start and Stop Time Parameters

These statements specify a start and stop date and/or time.

The formats are:

```
START TIME=time
START DATE=date
START DATE=date, TIME=time
STOP TIME=time
STOP DATE=date
STOP DATE=date, TIME=time
```

<b>Date/time Values</b>	<b>Explanation</b>
<i>hh:mm:ss</i>	Indicates hours:minutes:seconds.
<i>mm/dd/yyyy</i>	Indicates month/day/year.
<i>yyyy.ddd</i>	Indicates year/day in Julian format. For example, January 1, 2001 would be specified 2001.001.
<i>-number</i>	Indicates a number of days previous to the current date. For example, if on a Monday you want data from the weekend, you would specify: START DATE=-2 STOP DATE=-1

Examples:

```
START DATE=01/01/2001
START DATE=03/15/2001, TIME=08:00:00
START DATE=2001.001
START DATE=-2
STOP DATE=01/02/2001
STOP DATE=12/29/2001, TIME=16:00:00
```

## Record Type Parameter

This statement specifies the NetSpy SMF record type to be converted.

SMFTYPE=*n*

Operand	Explanation
SMFTYPE= <i>n</i>	Indicates the record number specified in the NetSpy installation using the statement SMF= <i>n</i> (OS/390 and z/OS only) or LOG= <i>n</i> .

Examples:

SMFTYPE 132  
SMFTYPE 128

## Print Parameters

This statement specifies which records are to be printed: either the original records or the converted records.

DUMP record, PRINT=*option*

Operand	Explanation
<i>record</i>	Indicates the type of record that should be printed. Can have one of the following values:
INPUT	Original NetSpy records
OUTPUT	Type 28 records
PRINT= <i>option</i>	Prints either of the following::
<i>nnn</i>	The first <i>nnn</i> bytes of each record
ALL	The entire record. This is the default.

Examples:

DUMP INPUT  
DUMP OUTPUT

## Error Parameters

This statement specifies how the program handles unsuccessfully converted records.

ERROR MAX=*n*, PRINT=*option*, OPTION=*option*

Operand	Explanation				
<b>MAX=<i>n</i></b>	Specifies the number of unsuccessfully converted records the program can encounter before aborting. You can specify a maximum of 99.				
<b>PRINT=<i>option</i></b>	Specifies that either of the following will be printed: <table border="1"><tbody><tr><td><i>number</i></td><td>The number of bytes of each unsuccessfully converted record</td></tr><tr><td>ALL</td><td>Each unsuccessfully converted record in its entirety</td></tr></tbody></table>	<i>number</i>	The number of bytes of each unsuccessfully converted record	ALL	Each unsuccessfully converted record in its entirety
<i>number</i>	The number of bytes of each unsuccessfully converted record				
ALL	Each unsuccessfully converted record in its entirety				
<b>OPTION=<i>option</i></b>	Writes one of the following to the data set specified on the SYSUT2 DD statement: <table border="1"><tbody><tr><td>PASS</td><td>Both the unsuccessfully and successfully converted records</td></tr><tr><td>DELETE</td><td>Only the converted records</td></tr></tbody></table>	PASS	Both the unsuccessfully and successfully converted records	DELETE	Only the converted records
PASS	Both the unsuccessfully and successfully converted records				
DELETE	Only the converted records				

Examples:

```
ERROR MAX=50  
ERROR MAX=5, PRINT=50  
ERROR OPTION=PASS
```

## DO Parameter

This statement restricts the type and number of records the program processes. Specify it *only* once in the JCL and *only* if you want to restrict the conversion to one type of record. This statement is primarily for test purposes.

```
DO TYPE=x,COUNT=n
```

Operand	Explanation
TYPE= <i>x</i>	Indicates the NetSpy record type to be processed. Specify one of the following values for <i>x</i> : <ul style="list-style-type: none"> <li>A, application</li> <li>C, gateway/session accounting</li> <li>D, APPN directory services</li> <li>E, MNPS application recovery</li> <li>F, CFS</li> <li>M, MNPS application</li> <li>N, NCP</li> <li>P, APPN topology</li> <li>R, RTP</li> <li>S, session start</li> <li>T, terminal</li> <li>U, session end</li> <li>▪ X, alert</li> </ul>
COUNT= <i>n</i>	Specifies how many output records to process. You can specify a maximum of 255. If you omit this parameter, all the records of the type you specify are printed.

Examples:

```
DO TYPE=A
DO TYPE=C,COUNT=100
DO COUNT=200
```

## Record Maps

This section shows how the Log records map to NPM type 28 records.

### SMF Record Header Map

The table below shows the SMF record header map.

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
0	Record descriptor word	0	SMF	SMF28LEN
		2	SMF	SMF28SEG
4	Flag byte	4	SMF	SMF28FLG
5	SMF Record type (x'28')	5	SMF	SMF28RTY
6	Time of Day	6	SMF	SMF28TME
	" " (1)	8	NAC	LNACCBCF
	" " (2)	10	NAC	LNACCECF
	" " (1)	8	NAD	LNADCBCF
	" " (2)	10	NAD	LNADCECF
	" " (1)	8	NAM	LNAMBTME
	" " (1)	8	SAA	LSAACBCF
	" " (2)	10	SAA	LSAACECF
	" " (1)	8	SSA	SSAACBCF
	" " (2)	10	SSA	SSAACECK
	" " (1)	8	SST	SSTBTME
	" " (2)	10	SST	SSTTETME
	" " (1)	8	STT	LSTTCBCF
	" " (2)	10	STT	LSTTCECF
	" " (1)	8	TRI	LTRICBCF
	" " (2)	10	TRI	LTRICECF
	" " (1)	8	ETH	LETHCBCF
	" " (2)	10	ETH	LETHCECF
	" " (1)	8	FRP	LFRPCBCF

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
	" " (2)	10	FRP	LRFPCECF
	" " (1)	8	CSL	LCSLCBCF
	" " (1)	10	CSL	LCSLCECF
	" " (2)	8	XLK	LXLKCBCF
	" " (1)	10	XLK	LXLKCECF
	" " (2)	8	XPU	LXPUCBCF
	" " (1)	10	XPU	LXPUCECF
	" " (2)	8	XVC	LXVCCBCF
	" " (1)	10	XVC	LXVCCECF
10	Date	10	SMF	SMF28DTE
	" " (1)	4	NAC	LNACCBSK
	" " (2)	C	NAC	LNACCESK
	" " (1)	4	NAD	LNADCBSK
	" " (2)	C	NAD	LNADCESK
	" " (1)	4	NAM	LNAMBDAT
	" " (2)	C	NAM	LNAMEDAT
	" " (1)	4	SAA	LSAACBSK
	" " (2)	C	SAA	LSAACESK
	" " (2)	4	SSA	SSAABSK
	" " (1)	C	SSA	SSAAESK
	" " (1)	4	SST	SSTTBDAT
	" " (2)	C	SST	SSTTEDAT
	" " (1)	4	STT	LSTTCBSK
	" " (2)	C	STT	LSTTCESK
	" " (1)	4	TRI	LTRICBSK
	" " (2)	C	TRI	LTRICESK
	" " (1)	4	ETH	LETHCBSK
	" " (2)	C	ETH	ELTHCESK
	" " (1)	4	FRP	LFRPCBSK
	" " (2)	C	FRP	LFRPCESK

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
	" " (1)	4	CSL	LCSLCBSK
	" " (2)	C	CSL	LCSLCESK
	" " (1)	4	XLK	LXLKCBSK
	" " (2)	C	XLK	LXLKCESK
	" " (2)	4	XPU	LXPUCBSK
	" " (1)	C	XPU	LXPUCESK
	" " (1)	4	XVC	LXVCCBSK
	" " (2)	C	XVC	LSVCCESK
14	System ID	14	SMF	SMF28SID
18	NetSpy/NPM record subtype (3)	16	SMF	SMF28RST
19	Number of entries for record			
20	Length of entry			
22	Major resource name	4	SCD	LSCDPNAM
30	Interval length (4)	14	NAC	LNACTIME
	" "	14	NAD	LNADTIME
	" "	14	TRI	LTRITIME
34	Zero			
35	Reserved			
38	Offset to first entry			
42	NetSpy release			
46	SYNC value (in 1/100 seconds)			
50	Flag			
51	Reserved			
52	APPL target level 1 or PIU distribution range 1	2E	BAN	BANPDR1
	" "	18	STT	LSTTBND1
	" "	68	STT	LSTTOPLT
	" "	84	STT	LSTHTLT
54	APPL target level 2 or PIU distribution range 2	30		BANPDR2
	" "	1C	BAN	LSTTBND2

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
	" " (5)	64	STT	LSTTOPHT
	" " (5)	80	STT	LSTTHTHT
			STT	
56	APPL target level 3 or PIU distribution range 3		BAN	BANPDR3
	" "	32	STT	LSTTBND3
	" " (5)	20	STT	LSTTOPHT
	" " (5)	64	STT	LSTTHTHT
		80		
58	APPL target level 4 or PIU distribution range 4	34	BAN	BANPDR4
	" "	24	STT	LSTTBND4
	" " (5)	64	STT	LSTTOPHT
	" " (5)	80	STT	LSTTHTHT
60	USER/NET target level 1 or PIU distribution range 5	36	BAN	BANPDR5
	" "	68	STT	LSTTOPLT
	" "	A0	STT	LSTTNLT
	" "			
62	USER/NET target level 2 or PIU distribution range 6	38	BAN	BANPDR6
	" " (5)	64	STT	LSTTOPHT
	" " (5)	9C	STT	LSTTNHT
	" " (5)			
64	USER/NET target level 3	64	STT	LSTTOPHT
	" " (5)	9C	STT	LSTTNHT
66	USER/NET target level 4	64	STT	LSTTOPHT
	" " (5)	9C	STT	LSTTNHT
68	Filler			

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
-----------------------------	-------------	-------------------------	---------	------

**Notes:**

- (1) The Begin time/date = NetSpy time/date - NetSpy interval
- (2) The End time/date = NetSpy time/date
- (3) The NetSpy type is converted to the corresponding NPM type.
- (4) In 1/100 seconds for NetSpy; in seconds for NPM
- (5) The highest value specified is used.

**Type A (Application) Record Map**

The table below shows the type A record in NetSpy and NPM.

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
0	Application name	4	CDS	SCDSPNAM
8	Application CID			
12	Last host response time			
16	Last network response time			
20	Worst host response time	70	SST	SSTHTMX
	" " (2)	54	SST	SSTOPMX
24	Worst network response time	8C	SST	SSTNTMX
	" "	A8	SST	SSTNAMX
	" " (2)	54	SST	SSTOPMX
28	Cumulative host response time	6C	SST	SSTHTTM
	" " (3)	50	SST	SSTOPTM
	" " (4)	60	SST	SSTOPSQ
	" " (5)	7C	SST	SSTHTSQ
32	Cumulative network response time	A4	SST	SSTNATM
	" " (3)	50	SST	SSTOPTM
	" " (4)	60	SST	SSTOPSQ
	" " (6)	B0	SST	SSTNASQ

<b>NetSpy Offset in Decimal</b>	<b>Description</b>	<b>NPM Offset in Hex</b>	<b>Section</b>	<b>Name</b>
36	Number of inputs	58	SST	SSTTOPCT
	" "	74	SST	SSTTHTCT
	" "	30	SSA	SSAASTBC
	" "	48	SSA	SSAASMBC
40	Number of outputs	24	SSA	SSAAPTBC
	" "	3C	SSA	SSAAPMBC
44	Number of network responses computed	90	SST	SSTTNTCT
	" "	AC	SST	SSTTNACT
	" "	1C	SSA	SSAASCBC
	" " (1) (9)	38	SST	SSTTTBK5
	" " (1) (10)	4C	SST	SSTTHBK5
	" " (1)	5C	SST	SSTTOPET
	" " (4)	60	SST	SSTTOPSQ
	" " (5)	7C	SST	SSTHTSQ
	" " (6)	B0	SST	SSTNASQ
	" " (7)	2C	SSA	SSAAPTMC
	" " (7)	44	SSA	SSAAPMMC
	" " (8)	38	SSA	SSAASTMC
	" " (8)	50	SSA	SSAASMMC
	Number of network responses computed * 3	20	SSA	SSAASCCC
48	Number of transactions terminated at the host			
52	Number of responses on target 1 (9)	28	SST	SSTTTBK1
	" " (10)	3C	SST	SSTTHBK1
	" " (1) (9)	38	SST	SSTTTBK5
	" " (1) (10)	4C	SST	SSTTHBK5
	" " (1)	5C	SST	SSTTOPET
56	Cumulative input length	34	SSA	SSAASTCC
	" "	4C	SSA	SSAASMCC
	" " (8)	38	SSA	SSAASTMC

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
	" " (8)	50	SSA	SSAASMMC
64	Cumulative output length	28	SSA	SSAAPTCC
	" "	40	SSA	SSAAPMCC
	" " (7)	2C	SSA	SSAAPTMC
	" " (7)	44	SSA	SSAAPMMC
72	Reserved			
108	Number of sessions monitored	18	SST	SSTTNLUS
		20	SST	SSTTSSCT
112	Target level 1			
116	Target level 2			
120	Target level 3			
124	Target level 4			
128	Number of responses on target 2 (9)	2C	SST	SSTTTBK2
	" " (10)	40	SST	SSTTHBK2
	" " (1) (9)	38	SST	SSTTTBK5
	" " (1) (10)	4C	SST	SSTTHBK5
	" " (1)	5C	SST	SSTTOPET
132	Number of responses on target 3 (9)	30	SST	SSTTTBK3
	" " (10)	44	SST	SSTTHBK3
	" " (1) (9)	38	SST	SSTTTBK5
	" " (1) (10)	4C	SST	SSTTHBK5
	" " (1)	5C	SST	SSTTOPET
136	Number of responses on target 4 (9)	34	SST	SSTTTBK4
	" " (10)	48	SST	SSTTHBK4
	" " (1) (9)	38	SST	SSTTTBK5
	" " (1) (10)	4C	SST	SSTTHBK5
	" " (1)	5C	SST	SSTTOPET
140	Max number of terminals that can be monitored			
142	Reserved			

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
145	Application flag			
146	Reserved			
	"ISTPUS"	1C	CDS	SCDSPSAP

**Notes:**

- (1) # network responses computed - (sum of # responses on targets 1-4)
- (2) Worst host + worst network response times
- (3) Cumulative host + cumulative network response times
- (4) (sum of cumulative response times/# network responses computed)\*\*2 \* # network responses computed
- (5) (cumulative host response time/# network responses computed)\*\*2 \* # network responses computed
- (6) (cumulative network response time/# network responses computed)\*\*2 \* # network responses computed
- (7) cumulative output length/# network responses computed
- (8) Cumulative input length/# network responses computed
- (9) If not Host
- (10) If Host

**Type C (Accounting) Record Map**

The table below shows the type C record in NetSpy and NPM.

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
0	Type of session record	2	BAS	BASCTF
1	Type of network accounting record (3)	3	BAN	BANDCTAC
2	Session start date (2)	60	BAS	BASNC PDT
	" " (5)	4	BAN	BANDTDTE
6	Session start time (2)	64	BAS	BASNCPTM
	" " (5)	8	BAN	BANDTTME
10	Session LU name	2C	ACD	LACDSNAM

<b>NetSpy Offset in Decimal</b>	<b>Description</b>	<b>NPM Offset in Hex</b>	<b>Section</b>	<b>Name</b>
	" " (1)	4	ACD	LACDPNAM
18	Session LU network address	17	BAS	BASLUA
24	Sequence number for this session	4	BAS	BASSEQN
	" "	2	BAN	BANDSEQ
26	Session partner network ID	24	ACD	LACDPNET
34	Session partner name (1)	4	ACD	LACDPNAM
42	Session SPLU network address	1D	BAS	BASPLUA
48	Line name	3C	ACD	LACDSLNK
56	Line address			
62	Link station name	34	ACD	LACDSPUN
	" " (1)	14	ACD	LACDPLNK
70	Link station network address	23	BAS	BASLKA
76	NCP of this LU	44	ACD	LACDSSAP
	" "	50	BAS	BASCNCP
84	NCP subarea			
88	Network ID for the LU	4C	ACD	LACDSNET
	" "	58	BAS	BASCNET
	" " (4)	3	BAN	BANDCPCD
96	CP qualified name	6	BAS	BASVPCN
113	Virtual route number	60	ACD	LACDVRN
114	Transmission priority	62	ACD	LACDTPF
115	Explicit route	5C	ACD	LACDERN
116	Reverse ER data	5E	ACD	LACDRERN
117	FID type	29	BAS	BASFIDT
118	Local origin address	2A	BAS	BASF2O
119	Local destination address	2B	BAS	BASF2D
120	Session stop date/interval date (6)	4	BAN	BANDTDTE
124	Session stop date/interval time (6)	8	BAN	BANDTTME
128	Total text PIUs received	E	BAN	BANDRTPC

<b>NetSpy Offset in Decimal</b>	<b>Description</b>	<b>NPM Offset in Hex</b>	<b>Section</b>	<b>Name</b>
132	Total text PIUs sent	12	BAN	BANDSTPC
136	Total text bytes received	16	BAN	BANDRTBC
140	Total text bytes sent	1A	BAN	BANDSTBC
144	Total control PIUs received	1E	BAN	BANDRCPC
148	Total control PIUs sent	22	BAN	BANDSCPC
152	Total control bytes received	26	BAN	BANDRCBC
156	Total control bytes sent	2A	BAN	BANDSCBC
160	Overflow counter for PIUs text received	2	BAN	BANDORTP
161	Overflow counter for PIUs text sent	2	BAN	BANDOSTP
162	Overflow counter for byte text received	2	BAN	BANDORTB
163	Overflow counter for byte text sent	2	BAN	BANDOSTB
164	Overflow counter for PIUs control text received	2	BAN	BANDORCP
165	Overflow counter for PIUs control text sent	2	BAN	BANDOSCP
166	Overflow counter for byte control text received	2	BAN	BANDORCB
167	Overflow counter for byte control text sent	2	BAN	BANDOSCB
168	Adjacent network ID of SLU (GWA)	38	BAS	BASADJS
176	Adjacent network ID of PLU (GWA)	30	BAS	BASADJP
184	Total PIUs received in distribution range 1	3A	BAN	BANRPDC1
188	Total PIUs received in distribution range 2	3C	BAN	BANRPDC2
192	Total PIUs received in distribution range 3	3E	BAN	BANRPDC3
196	Total PIUs received in distribution range 4	40	BAN	BANRPDC4
200	Total PIUs received in distribution range 5	42	BAN	BANRPDC5
204	Total PIUs received in distribution range 6	44	BAN	BANRPDC6
208	Total PIUs received in distribution range 7	46	BAN	BANRPDC7
212	Total PIUs sent in distribution range 1	48	BAN	BANSPDC1
216	Total PIUs send in distribution range 2	4A	BAN	BANSPDC2
220	Total PIUs sent in distribution range 3	4C	BAN	BANSPDC3
224	Total PIUs sent in distribution range 4	4E	BAN	BANSPDC4

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
228	Total PIUs send in distribution range 5	50	BAN	BANSPDC5
232	Total PIUs sent in distribution range 6	52	BAN	BANSPDC6
236	Total PIUs sent in distribution range 7	54	BAN	BANSPDC7
240	PIU distribution overflow bytes			
254	Session start record status			
255	Session flags	2C	BAS	BASF2F
	" "	2E	BAS	BASDSFLG
256	Alias name of SLU (GWA)	48	BAS	BASGASNM
264	Alias name of PLU (GWA)	40	BAS	BASGAPNM
272	NCP-PCID session ID value	64	ACD	LACDPCID
	" "	3	BAN	BANDCPCD
280	SNI date/time if available (2)	60	BAS	BASNDT
	"N"	6D	ACD	LACDXNET

**Notes:**

- (1) According to session type
- (2) SNI date/time if available, else session date/time
- (3) Flag set if accounting type = 'G'
- (4) Flag set if PCID is not blank
- (5) If session = 'S' (start)
- (6) If session = 'I' or 'E' (interval or end)

**Type D (APPN Directory Services)**

Netspy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
0	Number of resources successfully found in local database cache	84	VTT	VTTNFLDB
4	Number of resources successfully found from the central directory	88	VTT	VTTNFCDS

server				
8	Number of resources successfully found via domain broadcast	8C	VTT	VTTNFDMB
12	Number of resources successfully found via network broadcast	90	VTT	VTTNFNTB
16	Number of failed searches completed by receipt of a negative reply	94	VTT	VTTNFSNR
20	Number of times a network broadcast is not performed due to a negative cache entry	98	VTT	VTTNBCE
24	Number of matches where this node received a search request from another node and the requested resource was found	9C	VTT	VTTNSSRF
28	Number of matches where this node received a search request from another node and the requested resource was not found	A0	VTT	VTTNSSNF
32	Number of referrals received	A4	VTT	VTTNRCDS
36	Number of times a positive reply is received from an alternate central directory server	A8	VTT	VTTNPCDS
40	Number of times a negative reply is received from an alternate central directory server	AC	VTT	VTTNNCDS
44	Number of resources removed from local database due to value specified for either the DIRSIZE or DIRTIME start options	B0	VTT	VTTNRRGS
48	Number of adjacent nodes in a different sub-network	B4	VTT	VTTNANDS
52	Number of times a cache entry is discarded due to DIRSIZE maximum being reached	B8	VTT	VTTNCEDM
56	Number of registered resources	BC	VTT	VTTNUMRR
60	Current number of entries in the cache	C0	VTT	VTTNCACH

## Type E (MNPS Application Recovery)

<b>Netspy Offset in Decimal</b>	<b>Description</b>	<b>NPM Offset in Hex</b>	<b>Section</b>	<b>Name</b>
0	Application program name	2C	VMN	VMNAPPNM
8	Number of sessions recovered successfully by this VTAM	54	VMN	VMNNSRCV
12	Number of session recoveries attempted	58	VMN	VMNNSATT
16	Number of HPR pipes recovered successfully by this VTAM	5C	VMN	VMNNSRCV
20	Number of HPR pipes recoveries attempted	60	VMN	VMNNSATT
24	Total recovery time spent recovering sessions (TOD clock format)	64	VMN	VMNRCVTM

## Type F (CFS)

<b>Netspy Offset in Decimal</b>	<b>Description</b>	<b>NPM Offset in Hex</b>	<b>Section</b>	<b>Name</b>
0	Coupling facility structure name	34	VMN	VMNCFSNM
16	Coupling facility structure size in 1K blocks	50	VMN	VMNCFSIZ
20	Percentage of 1K blocks in use	4D	VMN	VMNCFPIK

## Type M (MNPS Application)

<b>Netspy Offset in Decimal</b>	<b>Description</b>	<b>NPM Offset in Hex</b>	<b>Section</b>	<b>Name</b>
0	Application program name	2C	VMN	VMNAPPNM
8	Coupling facility structure name	34	VMN	VMNCFSNM
24	Number of coupling facility	44	VMN	VMNNSCFWR

	writes for this application			
28	Number of bytes written to the coupling facility structure	48	VMN	VMNNBWCF

## Type N (NCP Resource) Record Map

The table below shows the type N (NCP resource) record in NetSpy and NPM.

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
0	NCP Name	44	NCD	LNCDSSAP
8	NCP Collection Interval	18	NAC	LNACCTIM
	" " (1)	1C	NAC	LNACFCC
12	Element type	2	NCD	LNCDRTYP
13	Used cycle count (1)	1C	NAC	LNACFCC
17	Free buffer queue length	20	NAC	LNACFBQ
19	Free buffer high watermark	24	NAC	LNACFBH
21	Free buffer low watermark	28	NAC	LNACFBL
23	NCP channel intermediate queue length	2C	NAC	LNACIQ
25	NCP channel hold queue length	30	NAC	LNACCHQ
27	Time in slowdown	34	NAC	LNACSL
29	Number of free buffers at slowdown	38	NAC	LNACSLM
31	Max free buffers	3C	NAC	LNACMXF
33	CCU cycle speed (1)	1C	NAC	LNACFCC
	" " (2)	40	NAC	LNACCYS
34	Reserved			
61	Delay value			
63	Reserved			
	"ISTPUS"	1C	NCD	LNCDPSAP

### Notes:

- (1) NCP collection interval-(Used cycle count/CCU cycle speed)
- (2) (CCU cycle speed/NCP collection interval)-Used cycle count

## Type N (Line, Controller, Terminal) Record Map

The table below shows the type N (line, controller, terminal) record in NetSpy and NPM.

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
0	Element Name (1)	2C	NCD	LNCDSNAM
		34	NCD	LNCDSPUN
		3C	NCD	LNCDSLNK
8	NCP collection interval	18	NAD	LNADCTIM
12	Element type	2	NCD	LNCDRTYP
13	Total messages sent	24	NAD	LNADPTBC
17	Total messages received	2C	NAD	LNADSTBC
21	Total bytes sent	28	NAD	LNADPTCC
25	Total bytes received	30	NAD	LNADSTCC
29	Outbound queue length	34	NAD	LNADROQ
31	Total poll count	38	NAD	LNADTPC
35	Positive poll count	3C	NAD	LNADPPC
39	Error count	40	NAD	LNADERR
41	Number of messages retransmitted	44	NAD	LNADRPC
45	Number of bytes retransmitted	48	NAD	LNADRBC
49	Line send speed	1C	NAD	LNADPLS
53	Line receive speed	20	NAD	LNADSLS
57	Network address for element/element address if ENA			
59	Element count for NCP entry			
61	Pause, in tenths of seconds			
63	REPLYTO			
65	MAXDATA			
67	MAXOUT			
68	PASSLIM			
69	PACING			
70	SERVLIM			

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
71	Resource subtype			
	"ISTPUS"	1C	NCD	LNCDPSPAP

**Note:** (1) Offset varies according to the element type (NetSpy-offset 12)

## Type N (X.25 NPSI) Record Map

The table below shows the type N (X.25 NPSI) record in NetSpy and NPM.

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
0	Element name	34	NCD	LNCDSPUN
		3C	NCD	LNCDSLNK
8	NCP collection interval in tenths of seconds	18	XLK	LXLKCTIM LXPUCTIM LXVCCTIM
12	Element type: X'46' - NPSI links X'48' - XI links X'24' - NPSI PUs X'25' - XI PUs X'26' - NPSI VCs	2	NCD	LNCDRTYP
13	Total number of I-frames sent	24	XLK	LXLKIFR
		84	XPU	LXPUPKTS
		7C	XVC	LXVCPKTS
17	Total number of I-frames received	2C	XLK	LXLKIFRR
		88	XPU	LXPUPKTR
		80	XVC	LXVCPKTR
21	Total number of bytes sent	28	XLK	LXLKBYTS
			XPU	LXPUBYTS
			XVC	LXVCBYTS

<b>NetSpy Offset in Decimal</b>	<b>Description</b>	<b>NPM Offset in Hex</b>	<b>Section</b>	<b>Name</b>
25	Total number of bytes received	30	XLK	LXLKBYTR
			XPU	LXPUBYTR
			XVC	LXVCBYTR
29	Outbound queue length	34	XLK	LXLKOBQL
			XPU	LXPUOBQL
			XVC	LXVCOBQL
31	Total number of RNR frames sent	7C	XLK	LXLKRNRS
			XPU	LXPURNRS
35	Total number of RNR frames received	80	XLK	LXLKRNR
			XPU	LXPURNRR
39	Total errors	40	XLK	LXLKTERR
			XPU	LXPUTERR
41	Number of I-frames retransmitted	44	XLK	LXLKXIFR
			XPU	LXPUXIFR
			XVC	LSVCXIFR
45	Number of bytes retransmitted	48	XLK	LXLKXBYT
			XPU	LXPUXBYT
			XVC	LXVCXBYT
49	Line send speed	1C	XLK	LXLKTLSP
			XPU	LXPUTLSP
			XVC	LXVCTLSP
53	Line receive speed	20	XLK	LXLKRSLP
			XPU	LXPURLSP
			XVC	LXVCRLSP
<b>X.25 MCH Line and XI Line Records Only</b>				
82	Total number of RR frames sent	84	XLK	LXLKRRS
86	Total number of RR frames received	88	XLK	LXLKRRR
<b>X.25 MCH PU and XI PU Records Only</b>				
82	Current number of VCs established	8C	XPU	LXPUCVC
84	Number of new VCs established this interval	90	XPU	LXPUNVC

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
86	Total number of outbound connections (calls)	94	XPU	LXPUOBCN
90	Total number of inbound connections (calls)	98	XPU	LXPUIBCN
94	Total number of outbound disconnections (clears)	9C	XPU	LXPUOBDN
98	Total number of inbound disconnections (clears)	A0	XPU	LXPUIBDN
102	Total number of INN-SHM connections	A4	XPU	LXPUSHMR
<b>X.25 VC Records Only</b>				
82	Total number of D-bit packets sent	84	XVC	LXVCPKSD
86	Total number of D-bit packets received	88	XVC	LXVCPKRD
90	Total number of M-bit packets sent	8C	XVC	LXVCPKSM
94	Total number of M-bit packets received	90	XVC	LXVCPKRM

## Type N (Token-Ring) Record Map

The table below shows the type N (token-ting) record in NetSpy and NPM.

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
0	Element name	2C	NCD	LNCDSNAM
		34	NCD	LNCDSPUN
		3C	NCD	LNCDSLNK
8	NCP collection interval (in tenths of seconds)	18	TRI	LTRICTIM
12	Element type: X'70' - LLINKs (logical links) X'71' - PLINKs (physical links)	2	NCD	LNCDRTYP
13	Transmit line speed	1C	TRI	LTRITLSP
17	Receive line speed	20	TRI	LTRIRLSP
21	IFRAMES send	24	TRI	LTRIIFRS
25	Total bytes sent	28	TRI	LTRIBYTS

<b>NetSpy Offset in Decimal</b>	<b>Description</b>	<b>NPM Offset in Hex</b>	<b>Section</b>	<b>Name</b>
29	IFRAMES received	2C	TRI	LTRIIFRR
33	Total bytes received	30	TRI	LTRIBYTR
37	Outbound queue length	34	TRI	LTRIOBQL
41	Reserved			
49	Total error count	40	TRI	LTRITERR
53	Retransmitted IFRAMES	44	TRI	LTRIXIFR
57	Retransmitted bytes	48	TRI	LTRIXBYT
61	Content flag 1	4C	TRI	LTRICON1
62	Reserved			
64	Content flag 4	4F	TRI	LTRICON4
65	Reserved			
66	Content flag 5	78	TRI	LTRICON5
67	Reserved			
70	Reserved	7C	TRI	LTRITFRS
74	VTAM switched definition PU name if available.	80	TRI	LTRITFRR
<b>Type X'70' (LLINK) Records Only</b>				
78	Reply time-outs	84	TRI	LTRIRPTO
<b>Type X'71' (PLINK) Records Only</b>				
78	Active connections	84	TRI	LTRIACTS
82	Congestion count	88	TRI	LTRICNGC
86	Time per byte send	8C	TRI	LTRITBS
90	Time per byte received	90	TRI	LTRITBR
94	Time per frame sent	94	TRI	LTRITFS
98	Time per frame received	98	TRI	LTRITFR
	"ISTPUS"	1C	NCD	LNDOPSAP

## Type N (TIC3) Record Map

The table below shows the type N (TIC3) record in NetSpy and NPM.

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
0	Element name	34	NCD	LNCDSPUN
		3C		LNCDSLNK
8	NCP collection interval in tenths of seconds	18	CSL	LCSLCTIM
12	Element type: X'4C' - Physical link X'28' - Physical unit	2	NCD	LNCDRTYP
13	I-frames sent	24	CSL	LCSLIFRS
17	I-frames received	2C	CSL	LCSLIFRR
21	Bytes sent	28	CSL	LCSLBYTS
25	Bytes received	30	CSL	LCSLBYTR
31	Total frames sent	7C	CSL	LCSLTFRS
35	Total frames received	80	CSL	LCSLTFRR
41	Retransmitted frames	44	CSL	LCSLXIFR
45	Retransmitted bytes	48	CSL	LCSLXBYT
49	Transmit line speed, if available	1C	CSL	LCSLLSPD
61	Time per byte sent, in nanoseconds	A4	CSL	LCSLBTPT
65	Time per byte received, in nanoseconds	A0	CSL	LCSLBRPT
<b>Extended Subtype X'40' Physical Link Records Only</b>				
82	Misaddressed frames received	8C	CSL	LCSLMFRD
86	Discarded frames	88	CSL	LCSLPDUD
90	Unrecognized frames	90	CSL	LCSLURFR
<b>Extended Subtype X'08' TIC3 Logical PU Records Only</b>				
82	Local busy occurrences	8C	CSL	LCSLLBOC
86	Rejected frames sent	90	CSL	LCSLRSFS
90	Rejected frames received	94	CSL	LCSLRSFR
94	LAN T2 timeouts	88	CSL	LCSLRPTO

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
<b>TIC Physical Links and TIC3 Logical PUs</b>				
98	Time per frame sent, in microseconds	9C	CSL	LCSLFTPT
102	Time per frame received, in microseconds	98	CSL	LCSLFRPT

## Type N (Ethernet Adapter) Record Map

The table below shows the type N (Ethernet Adapter) record in NetSpy and NPM.

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
0	Element name	3C	NCD	LNCDSLNK
8	NCP collection interval in tenths of seconds	18	ETH	LETHCTIM
12	Element type: For Ethernet physical link, X'48'	2	NCD	LNCDRTYP
13	I-frames sent	24	ETH	LETHIFRS
17	I-frames received	2C	ETH	LETHIFRR
21	Total bytes sent	28	ETH	LETHBYTS
25	Total bytes received	30	ETH	LETHBYTR
29	Outbound queue length	34	ETH	LETHOBQL
31	Total frames sent	7C	ETH	LEHTFRS
35	Total frames received	80	ETH	LEHTFRR
82	Congestion count	84	ETH	LETHCNGC
86	Transmission deferred count	88	ETH	LEHTTDD
90	One collision count	8C	ETH	LETHOCO
94	Multiple collision count	90	ETH	LETHMCO

## Type N (Frame Relay) Record Map

The table below shows the type N (Frame Relay) record in NetSpy and NPM.

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
0	Element name	34 3C	NCD	LNCDSPUN LNCDSLNK
8	NCP collection interval in tenths of seconds	18	FRP	LF RPCTIM
12	Element type: X'49' - Frame Relay physical links X'49' - Frame Relay logical links X'2A' - Frame Relay LMI stations X'29' - Frame Relay physical stations	2	NCD	LNC DR TYP
13	I-frames sent	24	FRP	LF RP IFRS
17	I-frames received	2C	FRP	LF RP IFRR
21	Total bytes sent	28	FRP	LF RP BYTS
25	Total bytes received	30	FRP	LF RP BYTR
29	I-frames on link outbound queue	34	FRP	LF RP OBQL
31	Total frames sent	7C	FRP	LF RP TFRS
35	Total frames received	80	FRP	LF RP TFRR
41	Number of frames retransmitted	44	FRP	LF RP XIFR
45	Number of bytes retransmitted	48	FRP	LF RP XBYT
<b>Frame Relay Physical Link Records Only</b>				
82	Number of active logical connections	84	FRP	LF RP ACTS
84	Number of frames with forward congestion	88	FRP	LF RP LFC
88	Number of frames with backward congestion	8C	FRP	LF RP LBC
92	Number of frames discarded	90	FRP	LF RP PDF
<b>Frame Relay Logical Link Records Only</b>				
82	Number of reply timeouts	84	FRP	LF RP TO
86	Number of frames with forward congestion	88	FRP	LF RP LFC

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
90	Number of frames with backward congestion	8C	FRP	LFRPLBC
<b>Frame Relay LMI Station Records Only</b>				
82	Number of frames discarded	90	FRP	LFRPPDF
<b>Frame Relay Physical Station Records Only</b>				
82	Number of frames with forward congestion	88	FRP	LFRPLFC
86	Number of frames with backward congestion	8C	FRP	LFRPLBC
90	Number of frames discarded	90	FRP	LFRPPDF

### Type P (APPN Topology)

Netspy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
0	Number of routes calculated using an existing tree	2C	VTT	VTTNRCET
4	Number of routes calculated using a modified tree	30	VTT	VTTNRCMT
8	Number of routes calculated using a new tree	34	VTT	VTTNRCNT
12	Number of topology database updates (TDUs) originated by this node	38	VTT	VTTNTDUO
16	Number of TDUs propagated by this node	3C	VTT	VTTNTDUP
20	Number of TDUs received by this node resulting in a topology database update	40	VTT	VTTNTDUR
24	Number of TDUs received by this node and discarded by this node for normal reasons. Resource sequence number (RSN) is valid, but data already seen	44	VTT	VTTNTRDN

28	Number of TDUs received by this node and discarded because the RSN is not valid. (TDU is rebroadcast)	48	VTT	VTTNTRDR
32	Number of TDUs received by this node and discarded because of data inconsistency. (TDU is rebroadcast)	4C	VTT	VTTNTRDI
36	Number of network nodes in the topology database	50	VTT	VTTNNNTD
40	Number of end nodes in the topology database	54	VTT	VTTNENTD
44	Number of unidirectional TGs in the topology database	58	VTT	VTTNUGTD
48	Number of TG failures at this node	5C	VTT	VTTNTGFN
52	Number of dynamic PU allocations	60	VTT	VTTNDPUA
56	Number of times a routing tree was discarded due to the tree cache becoming full	64	VTT	VTTNRTDF
60	Current number of trees in the tree cache	68	VTT	VTTNCTTC
64	Number of virtual nodes in the topology database	6C	VTT	VTTNVNTD
68	Number of central directory server nodes in the topology database	70	VTT	VTTNCNTD
72	Number of interchange nodes in the topology database	74	VTT	VTTNINTD
76	Number of end nodes connected to this node	78	VTT	VTTNENCN
80	Number of network nodes connected to this node	7C	VTT	VTTNNNCN
84	Number of virtual nodes connected to this node	80	VTT	VTTNVNCN

## Type R (VTAM RTP)

<b>Netspy Offset in Decimal</b>	<b>Description</b>	<b>NPM Offset in Hex</b>	<b>Section</b>	<b>Name</b>
0	RTP physical unit	3C	VRT	VRTPU
8	Remote network ID	44	VRT	VRTRNID
16	Remote CP name	4C	VRT	VRTRCPN
24	RTP state X'80' - ACTIVE X'40' - INACTIVE X'20' - NORMAL	7	VRT	VRTSTATE
25	Round trip delay	7C	VRT	VRTRTD
29	Number of bytes sent over the RTP	80	VRT	VRTNBSNT
33	Number of bytes received over the RTP	84	VRT	VRTNBREC
37	Number of PIUs that were segmented sent over the RTP	88	VRT	VRTPIUFS
41	Number of PIUs that were not segmented sent over the RTP	94	VRT	VRTPIUNS
45	Number of PIUs that were segmented received over the RTP	98	VRT	VRTPIUFR
49	Number of PIUs that were not segmented received over the RTP	A4	VRT	VRTPIUNR
53	Number of HPR path switch attempt initiated by other RTP endpoint	AC	VRT	VRTPSAOE
55	Number of HPR path switch attempts due to operator or VTAM command	B0	VRT	VRTPSAOP
57	Number of HPR path switch attempts due to any other failure (such as link failure or node failure)			
59	Number of HPR path switch attempts due to operator or VTAM command that were unsuccessful	B4	VRT	VRTUPSOP

61	Number of HPR path switch attempts due to any other failure (such as link failure or node failure) that were unsuccessful			
63	Number of active LU-LU sessions using the RTP	B8	VRT	VRTLULUS
67	Number of times that back pressure has been applied due to HPR path switch	C2	VRT	VRTBPAPS
69	Number of time back pressure has been applied queue depth exceeded	C4	VRT	VRTBPAQD
71	Number of times back pressure applied due to storage shortage			
73	Number of retransmitted NLPs	C8	VRT	VRTRENLP

### Type S (Terminal Session) Record Map

The table below shows the type S record in NetSpy and NPM.

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
0	Terminal name	2C	SCD	LSCDSNAM
8	Terminal CID			
12	Session type			
16	Reserved			
20	Last host response time			
24	Last network response time			
28	Worst host response time	70	STT	LSTHTMX
	" " (2)	54	STT	LSTTOPMX
32	Worst network response time	A8	STT	LSTTNAMX
	" "	8C	STT	LSTINTMX
	" " (2)	54	STT	LSTTOPMX

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
36	Cumulative host response time	6C	STT	LSTTHTTM
	" " (3)	50	STT	LSTTOPTM
	" " (5)	7C	STT	LSTHTSQ
	" " (6)	60	STT	LSTTOPSQ
40	Cumulative network response time	A4	STT	LSTTNATM
	" "	88	STT	LSTINTM
	" " (6)	B0	STT	LSTINASQ
	" " (3)	50	STT	LSTTOPTM
	" " (6)	60	STT	LSTTOPSQ
	" " (6)	98	STT	LSTNTSQ
44	Number of inputs	58	STT	LSTTOPCT
	" "	74	STT	LSTHTCT
	" "	B4	STT	LSTTNOCT
	" "	30	SAA	LSAASTBC
	" "	48	SAA	LSAASMBC
46	Number of outputs	24	SAA	LSAAPTBC
	" "	3C	SAA	LSAAPMBC
48	Number of network responses computed		STT	LSTINTCT
	" "	90	STT	LSTTINACT
	" "	AC	SAA	LSAASCBC
	" " (1) (9)	1C	STT	LSTTBK5
	" " (10)	38	STT	LSTTHBK5
	" " (10)	4C	STT	LSTTOPET
	" " (1) (6)	5C	STT	LSTHTTET
	" " (5)	78	STT	LSTTOPSQ
	" " (6)	60	STT	LSTHTSQ
	" " (6)	7C	STT	LSTNTSQ
	" "	98	STT	LSTINASQ
	" " (7)	B0	STT	LSTTNOCT
	" " (10)	B4	STT	LSTINTET

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
	" " (8)	94	SAA	LSAAPTMC
	" " (8)	2C	SAA	LSAASTMC
	" " (7)	38	SAA	LSAASMMC
	" " (8)	50	SAA	LSAAPMMC
	Number of network responses computed * 3	44 20	SAA	LSAASCCC
50	Number of responses on target 1 (9)	3C	STT	LSTTHBK1
	" " (10)	4C	STT	LSTTHBK5
	" " (10)	5C	STT	LSTTOPET
	" " (10)	78	STT	LSTTHTET
	" "	28	STT	LSTTTBK1
	" " (10)	38	STT	LSTTTBK5
52	Cumulative input length	34	SAA	LSAASTCC
	" "	4C	SAA	LSASSMCC
	" " (8)	38	SAA	LSAASTMC
	" " (8)	50	SAA	LSAASMMC
56	Cumulative output length	28	SAA	LSAAPTCC
	" "	40	SAA	LSASAPMCC
	" " (7)	2C	SAA	LSAAPTMC
	" " (7)	44	SAA	LSAAPMMC
60	Number of responses on target 2	40	STT	LSTTHBK2
	" " (10)	4C	STT	LSTTHBK5
	" " (10)	5C	STT	LSTTOPET
	" "	2C	STT	LSTTTBK2
	" " (10)	38	STT	LSTTTBK5
	" " (10)	5C	STT	LSTTOPET
62	Number of responses on target 3	44	STT	LSTTHBK3
	" " (10)	4C	STT	LSTTHBK5
	" " (10)	5C	STT	LSTTOPET
	" "	30	STT	LSTTTBK3

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
	" " (10)	38	STT	LSTTTBK5
	" " (10)	5C	STT	LSTTOPET
64	Number of responses on target 4	48	STT	LSTTHBK4
	" " (10)	4C	STT	LSTTHBK5
	" " (10)	5C	STT	LSTTOPET
	" "	34	STT	LSTTTBK4
	" " (10)	38	STT	LSTTTBK5
	" " (10)	5C	STT	LSTTOPET
67	Flags			
69	Virtual Route	60	SCD	LSCDVRN
70	Reserved			
71	Flag			
	"ISTPUS"	1C	SCD	LSCDPSAP
	"N"	6D	SCD	LSCDXNET

**Notes:**

- (1) # network responses computed - (sum of Global NTARGET/UTARGETs 1-4)
- (2) Worst host + worst network response times
- (3) Cumulative host + cumulative network response times
- (4) (Sum of cumulative response times/# network responses computed)\*\*2 \* # network responses computed
- (5) (Cumulative host response time/# network responses computed)\*\*2 \* # network responses computed
- (6) (Cumulative network response time/# network responses computed)\*\*2 \* # network responses computed
- (7) Cumulative output length/# network responses computed
- (8) Cumulative input length/# network responses computed
- (9) User Targets only
- (10) # network responses computed - (sum of # responses on targets 1-4)

## Type T and U (Terminal) Record Map

The table below shows the type T and U (Terminal) record map.

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
0	Terminal name	2C	SCD	LSCDSNAM
8	Terminal CID			
12	Reserved			
20	Last host response time			
24	Last network response time			
28	Worst host response time (11)	70	STT	LSTHTMX
	" " (2) (11)	54	STT	LSTTOPMX
32	Worst network response time (11)	A8	STT	LSTTNAMX
	" " (11)	8C	STT	LSTINTMX
	" " (2) (11)	54	STT	LSTTOPMX
36		6C	STT	LSTHTTM
		50	STT	LSTTOPTM
		7C	STT	LSTHTSQ
		60	STT	LSTTOPSQ
40	Cumulative network response time (11)	A4	STT	LSTTNATM
	" " (11)	88	STT	LSTINTTM
	" " (6) (11)	B0	STT	LSTTNASQ
	" " (3) (11)	50	STT	LSTTOPTM
	" " (6) (11)	60	STT	LSTTOPSQ
	" " (6) (11)	98	STT	LSTINTSQ
44	Number of inputs (11)	58	STT	LSTTOPCT
	" " (11)	74	STT	LSTHTCT
	" " (11)	B4	STT	LSTTNOCT
	" "	30	SAA	LSAASTBC
	" "	48	SAA	LSAASMBC

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
46	Number of outputs	24	SAA	LSAAPTBC
	" "	3C	SAA	LSAAPMBC
48	Number of network responses computed (11)		STT	LSTINTCT
	" " (11)	90	STT	LSTINACT
	" "	AC	SAA	LSAASCBC
	" " (1) (9) (11)	1C	STT	LSTTTBK5
	" " (10) (11)	38	STT	LSTTHBK5
	" " (10) (11)	4C	STT	LSTTOPET
	" " (1) (6) (11)	5C	STT	LSTTHTET
	" " (5) (11)	78	STT	LSTTOPSQ
	" " (6) (11)	60	STT	LSTTHTSQ
	" " (6) (11)	7C	STT	LSTINTSQ
	" " (11)	98	STT	LSTTNASQ
	" " (7) (11)	B0	STT	LSTTNOCT
	" " (10) (11)	B4	STT	LSTINTET
	" " (8)	94	SAA	LSAAPTMC
	" " (8)	2C	SAA	LSAASTMC
	" " (7)	38	SAA	LSAASMMC
	" " (8)	50	SAA	LSAAPMMC
	Number of network responses computed * 3	44	SAA	LSAASCCC
		20		
50	Number of responses on target 1 (9)(11)	3C	STT	LSTTHBK1
	" " (10) (11)	4C	STT	LSTTHBK5
	" " (10) (11)	5C	STT	LSTTOPET
	" " (10) (11)	78	STT	LSTTHTET
	" " (11)	28	STT	LSTTTBK1
	" " (10) (11)	38	STT	LSTTTBK5

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
52	Cumulative input length	34	SAA	LSAASTCC
	" "	4C	SAA	LSASSMCC
	" " (8)	38	SAA	LSAASTMC
	" " (8)	50	SAA	LSAASMMC
56	Cumulative output length	28	SAA	LSAAPTCC
	" "	40	SAA	LSAAPMCC
	" " (7)	2C	SAA	LSAAPTMC
	" " (7)	44	SAA	LSAAPMMC
60	Number of responses on target 2 (11)	40	STT	LSTTHBK2
	" " (10) (11)	4C	STT	LSTTHBK5
	" " (10) (11)	5C	STT	LSTTOPET
	" " (11)	2C	STT	LSTTTBK2
	" " (10) (11)	38	STT	LSTTTBK5
	" " (10) (11)	5C	STT	LSTTOPET
62	Number of responses on target 3 (11)	44	STT	LSTTHBK3
	" " (10) (11)	4C	STT	LSTTHBK5
	" " (10) (11)	5C	STT	LSTTOPET
	" " (11)	30	STT	LSTTTBK3
	" " (10) (11)	38	STT	LSTTTBK5
	" " (10) (11)	5C	STT	LSTTOPET
64	Number of responses on target 4 (11)	48	STT	LSTTHBK4
	" " (10) (11)	4C	STT	LSTTHBK5
	" " (10) (11)	5C	STT	LSTTOPET
	" " (11)	34	STT	LSTTTBK4
	" " (10) (11)	38	STT	LSTTTBK5
	" " (10) (11)	5C	STT	LSTTOPET
67	Flags			
69	Virtual Route	60	SCD	LSCDVRN
70	Reserved			
71	Flag			

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
72	Line name for this LU	3C	SCD	LSCDSLNK
80	Cluster controller name for this LU	34	SCD	LSCDSPUN
88	User ID for session LU			
96	Global NTARGET/UTARGETx #1 (9) (11)	28	STT	LSTTTBK1
	" " (1) (11)	38	STT	LSTTTBK5
	" " (10) (11)	5C	STT	LSTTOPET
	" " (1) (11)	94	STT	LSTTNTET
98	Global NTARGET/UTARGETx #2 (9) (11)	2C	STT	LSTTTBK2
	" " (1) (11)	38	STT	LSTTTBK5
	" " (10) (11)	5C	STT	LSTTOPET
	" " (1) (11)	94	STT	LSTTNTET
100	Global NTARGET/UTARGETx #3 (9) (11)	30	STT	LSTTTBK3
	" " (1) (11)	38	STT	LSTTTBK5
	" " (10) (11)	5C	STT	LSTTOPET
	" " (1) (11)	94	STT	LSTTNTET
102	Global NTARGET/UTARGETx #4 (9) (11)	34	STT	LSTTTBK4
	" " (1) (11)	38	STT	LSTTTBK5
	" " (10) (11)	5C	STT	LSTTOPET
	" " (1) (11)	94	STT	LSTTNTET
	"ISTPUS"	1C	SCD	LSCDPSAP
	"N"	6D	SCD	LSCDXNET

**Notes:**

- (1) # network responses computed – (sum of Global NTARGET/UTARGETs 1-4)
- (2) Worst host + worst network response times
- (3) Cumulative host + cumulative network response times
- (4) (Sum of cumulative response times/# network responses computed)\*\*2 \* # network responses computed
- (5) (Cumulative host response time/# network responses computed)\*\*2 \* # network responses computed
- (6) (Cumulative network response time/# network responses computed)\*\*2 \* # network responses computed

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
(7)	Cumulative output length/# network responses computed			
(8)	Cumulative input length/# network responses computed			
(9)	User Targets only			
(10)	# network responses computed – (sum of # responses on targets 1-4)			
(11)	For LU 6.2 sessions, no response time data is available in the STT section. These fields will contain a value of 0 (zero).			

## Type X (General Alert) Record Map

The table below shows the type X (Alert) record in NetSpy and NPM.

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
0	Time alert was recorded	0C	NAM	LNAMEDAT
		10	NAM	LNAMETIM
		0C	NAC	LNACCESK
		10	NAC	LNACCECF
		0C	NAD	LNADCESK
		10	NAD	LNADCECF
8	Name of monitor recording event			
16	NSXNAME (name of cross-domain NetSpy that issued the alert)			
24	Resource name (1)	2C	NCD	LNCDSNAM
		34	NCD	LNCDSPUN
		3C	NCD	LNCDSLNK
32	User-specified description of alert			
80	Resource type	2	NCD	LNCDRTYP
81	Routing destination flags			
82	Number of variable-value pairs			
84	Variable-value pairs	19	NAM	LNAMTYP

NetSpy Offset in Decimal	Description	NPM Offset in Hex	Section	Name
	■ 1 - Variable type	18	NAM	LNAMFLG
	■ 1 - Operator type (2)	20	NAM	LNAMLIM
	■ 4 - User-specified threshold	1C	NAM	LNAMDAT
	■ 4 - Current reported value			
	"ISTPUS"	1C	NCD	LNCDPSAP

**Notes:**

(1) Offset varies according to resource type.

(2) If 'equal' (x'80') in NetSpy record, set to 'above' in Type 28 record.

---

# Using Database Utilities

NetSpy's batch reports do not support pulling data from Database records. Instead, you can use the database conversion utility to convert the records from a database format to the standard SMF format.

## Converting Database Records to Log Format

NSYDBCVC Utility

To run the database conversion utility, edit and submit the JCL in the NSYDBCVC member of the *dsnpref.NYvvv.CNTL* data set. Refer to the instructions in the member, as shown in the following JCL.

Specify the DBPARMS DD statement only if you are using Datacom/DB and have specified a database ID other than 619. The statement is not needed if you are using Datacom/AD.

The optional DBSTATS DD statement causes message NSY2406 to be issued, which contains a one-line summary of I/O activity for each table in the database.

```
//NSYDBCVC JOB 1,NS-DBCVC,CLASS=A,MSGCLASS=H
//*****
/* THIS JOB WILL CREATE SMF RECORDS FROM THE NETSPY DATABASE
/*
/* THE PARAMETERS PASSED INDICATE THE SPECIFIC NETSPY LOG RECORD
/* TYPE(S) TO BE EXTRACTED, GROUPED BY TYPE, AND IN WHAT ORDER THE
/* TYPE(S) SHOULD BE WRITTEN TO THE LOG FILE.
/*
/* OPTIONALLY, A START DATE AND/OR A STOP DATE MAY BE SPECIFIED, IN
/* ONE OF THE FOLLOWING FORMS:
/*   PARM='START=YYYYMMDD'           <-- STANDARD DATE
/*   PARM='START=YYYYDDD'           <-- JULIAN DATE
/*   PARM='START=-NNN'               <-- RELATIVE DATE
/*   PARM='STOP=YYYYMMDD'           <-- STANDARD DATE
/*   PARM='STOP=YYYYDDD'           <-- JULIAN DATE
/*   PARM='STOP=-NNN'               <-- RELATIVE DATE
/* THE EXTRACTION WILL IGNORE ALL DATABASE DATA CREATED BEFORE THE
/* START DATE AND CREATED ON OR AFTER THE STOP DATE.
/*
/* START DATE, STOP DATE, AND SPECIFIC RECORD TYPES MAY BE
/* SPECIFIED TOGETHER, AS LONG AS ALL RECORD TYPES FOLLOW THE
/* DATE SPECIFICATIONS.  FOR EXAMPLE,
/*   PARM='START=-3 STOP=-0 A'
/* WILL SELECT ALL 'APPLICATION' DATA CREATED IN THE PRIOR 3 DAYS.
/*
/* IF NO PARAMETERS ARE PASSED, ALL TYPES WILL BE CONVERTED AND
/* WRITTEN TO THE LOG, ORDERED BY TYPE, AND CHRONOLOGICALLY
```

```
//* WITHIN TYPE.
//*
//*
//*
//*****
//NSYBCV EXEC PGM=NSYBCV <-- ALL TYPES
//*NSYBCV EXEC PGM=NSYBCV,PARM='A B C N T U V X' <-- SELECT TYPES
//STEPLIB DD DISP=SHR,DSN=dsnpref.NYvvv.NYLOAD <-- MODIFY
// DD DISP=SHR,DSN=YOUR.DATACOM.CUSTOM.LOAD <-- MODIFY
// DD DISP=SHR,DSN=YOUR.DATACOM.LOAD <-- MODIFY
//SYSUDUMP DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSTEM DD SYSOUT=*
//LOG DD DISP=SHR,DSN=dsnpref.NYvvv.LOGDUMP <-- MODIFY
//DBPARMS DD *
DBID 619 <-- MODIFY
/*
//
```

## Converting Log Records to Database Format

NSYDBLD Utility      The NSYDBLD utility performs the reverse process of the NSYBDCV utility. It converts data from NetSpy Log format into Database format. To run this job, edit and submit the JCL in member NSYDBLD of the *dsnpref*.NYvvv.CNTL data set.

## Purging the Database

NSYDCP Utility      The NSYDCP utility purges the Database. Run this job regularly to delete data before the Database becomes full. For example, you can run the job daily, purging all data that is older than seven days. To run this job, edit and submit the JCL in member NSYDCP of the *dsnpref*.NYvvv.CNTL data set.

# Installing the APPN Monitor (Optional)

The APPN Monitor allows you to monitor Advanced Peer-to-Peer Networking (APPN) and multinode persistent session (MNPS) data.

## Install the APPN Monitor

To install the APPN monitor:

1. Specify the PMI statement in NetSpy's INITPRM file.
2. Install Netspy's VTAM performance measurement interface exit routine, NSYPMXIT.

The NSYPMXIT exit resides in library *dsnpref.NYvvv.EXIT.LOAD*. Do **one** of the following:

- Move the exit from that library to a user-defined library already in the VTAMLIB concatenation in your VTAM start up.
  - APF-authorize *dsnpref.NYvvv.EXIT.LOAD* and include it in the VTAMLIB concatenation.
3. Add Netspy's performance monitor application to VTAM.

The application name must match the ACBNAME specified on the PMI statement in Netspy's INITPRM file. The VTAM definition should look similar to:

```
NSYPMI APPL AUTH=(CNM,SPO)
```

NetSpy will communicate with VTAM, and instruct VTAM which exit to use, based on information in the PMI control parameter in the INITPRM data set. If you do not specify an exit name in the PMI control parameter, the default is NSYPMXIT.

See the IBM *SNA Customization Guide* for more information on the functionality and use of the PMI Exit.



# System Requirements

---

## Virtual Storage Amounts

NetSpy SNA Services will use the following amounts of virtual storage in the NetSpy address space for OS/390 and z/OS operating systems.<sup>1</sup> Storage amounts are listed by the NetSpy SNA Services feature. All storage is allocated below the 16MB line unless otherwise noted.

### Base Storage

1900K

### Batch Reporting

The amount of storage required for each increment of the MAX#RPT parameter differs depending on the type of reports you are requesting:

- For each summary all report, 15272 bytes
- For each summary/graph report with RBUCKETS specified, 8872 bytes
- Other summary/graph reports, 5672 bytes

You can specify up to 5,000 resource names or EXDAYS parameters in summary, graph, or print reports. Each specification requires 10 bytes.

**In OS/390 and z/OS, and MVS/ESA**, this storage will be allocated above the 16MB line, provided extended storage is available. You can use this figure to determine if a large value of the MAX#RPT parameter is the cause of a GETMAIN failure.

---

<sup>1</sup> For MVS/ESA systems, also see “CSA Storage Amounts” because some storage areas have been moved from CSA to NetSpy private storage.

## Collection Enhancements

$180K + (\text{MAXLU} \times 24) + (\text{MAXNONCP} + (2 \times \text{MAXNCPSZ})) \times 588 + (\text{MAXOPER} \times 4480) + (228 \times \text{\#TCP/IP connections})$

464 times #LUs monitored and/or collected on and/or displayed (that is, Summary, Delta) using collection enhancements.

(496 + 196) times #applications monitored and/or collected on and/or displayed.

$(172 + 96) \times \text{\#virtual routes being monitored and/or collected on and/or displayed.}$

**Note:** For the second enhancement point, this storage is dynamic and is freed when LU monitor is deleted, LU collection stopped, or LU display ended.

## Dynamic Reconfiguration Storage

For each NCP:  $16 + (80 (\text{NCPENT}) \times (\text{\#LUDRPOOL entries} + \text{\#PUDRPOOL entries}))$ .

**In OS/390 and z/OS, and MVS/ESA running in ESA mode,** this storage will be allocated above 16 MB in virtual storage, provided extended storage is available.

## Graphic Alerts

$3K + (\text{GMAXENT} \times (68 + (\text{\#partitions} \times 12) + (\text{\#variables} \times 4)))$ , where #partitions is the number of graph partitions that NetSpy creates to display the selected variables in graphic alerts. “#partitions” is calculated as follows:

Add 1 for each resource type selected in graphic alerts.

If a resource type has more than 3 variables selected, take the number of variables for that resource, divide by 3, and round up to the nearest integer. Subtract 1 from the integer and add the result to the “#partitions.”

“#variables” is the number of variables selected on the graphic alerts selection menu.

The maximum storage in bytes used for a graphic alerts user occurs when all variables are selected. The amount is calculated as:

$3K + (\text{GMAXENT} \times 444)$

**In OS/390 and z/OS, and MVS/ESA running in ESA mode,** this storage will be allocated above 16 MB in virtual storage, provided extended storage is available.

## NCP Definitions

Major Node size = ((header length of 192) + ((# entries) x (element length of 80))).

**For NCPs:** # entries = RRTCOUNT - (#RRT NAU) - (blank RRT entries) - (zero RRT entries). This is equal to the number of non-NAU RRT (Network Addressable Unit Resource Resolution Table) entries.

**For non-NCPs:** # entries = # of minor nodes (for example, switched PUs) defined in the VTAMLST definition.

MAXNCPSZ is the number of lines, controllers, and terminals in the largest NCP defined to NetSpy. See the section [INITPRM Parameter Descriptions](#) in the chapter "Defining Initialization Parameters."

#NCP dynamic resources =

#AUXADDR  
 + #ADDSESS (on BUILD statement)  
 + NUMBER (on LUPPOOL statement)  
 + NUMILU + NUMTYP1 + NUMTYP2 (on LUDRPOOL statement)  
 + NUMBER + MAXLU (on PUDRPOOL statement)  
 + RESSCB (on LINE statement)

The actual size of the NCP database is compared to the entire area obtained for the database. If the difference is greater than 1K, an area that is the exact size used for the database is obtained, the database is moved into the new area, and the old area is freed. It is possible to have two large areas of storage obtained at the same time before the original is deleted.

**Note:** During the DEFINE of the NCP, the RRT is loaded to verify addresses and is then released.

## NCP Statistics

One statistics buffer is obtained for each collectable resource.

**Normal Statistics Buffers (for NCP LUs and terminals only):**  
 ((MAXNOCOL) x (buffer length of normal stat buffer(88)))

where:

MAXNOCOL = (MAXNONCP x 500)  
 MAXNONCP = INITPRM specification

**Extended Statistics Buffers (for all NCP resources except LUs and terminals):**  
 (((# extended resources) x (extended buffer length(272))) + (extended stat buffer control area (16)))

where:

#extended resources =  
X.25 collectable resources=  
+ #NTRI collectable resources  
+ #Frame Relay collectable resources  
+ #Ethernet Adapter collectable resources  
+ #TIC3 collectable resources  
+ #NCP control block resources for NCP V7R1 or higher  
+ #LINE collectable + NPA collectable

#NCP control block resources (NCP V7R1 or higher) = 27 + (# adjacent network x 3)  
27 single network pools  
3 adjacent network-dependent pools

X.25 collectable resources =  
+1 for a control area  
+2 for each MCH line  
+2 for each MCH PU  
+ NPPVCN on the X.25 MCH statement (# of concurrent collectable VCs)

#NTRI collectable resources =  
+1 for each NTRI line  
+1 for each NTRI PU

#Frame Relay collectable resources =  
+1 for each physical line  
+1 for each logical line (NCP V6.2)  
+1 for each PU (NCP V6.2)

#Ethernet Adapter collectable resources =  
+1 for each physical line

#TIC3 collectable resources =  
+1 for each physical LINE with NPACOLL=(YES,EXT)  
+1 for each logical PU with NPACOLL=(YES,EXT)

**Five NCP buffers** for writing to log files: 5 x 11472

**Maximum collectable resources** = ((MAXCOLL in NCP generation + (#dynamic resources)).

If MAXCOLL is not specified in the NCP generation:

Max collectable resources = ((10) + (1 for each line) + (#NCP dynamic resources, see above))

## Network Accounting

$((\#NCP \text{ network accounting resources}) + (\#dynamic \text{ NCP resources} - \#dynamic \text{ PU resources}) \times (\text{network accounting entry length}(208)) + (\text{network accounting control area}(48)))$

where:

$\#NCP \text{ accounting resources} = ((1 \text{ for each LU}) + (1 \text{ for each terminal}))$

$\#NCP \text{ dynamic resources} = \text{see above.}$

## Gateway Accounting Storage

$((HSBPOOL + SESSLIM + NUMADDR + NUMSESS) + (\text{number of NCP network accounting resources}) \times (\text{accounting entry length}(208)) + (\text{accounting control area}(48)))$ .

**Note:** HSBPOOL, SESSLIM, NUMADDR, and NUMSESS are from the BUILD statement.

## NetSpy-to-NetSpy, Collection Enhancements, and Alerts

Default Allocation:

$((\text{MAXNONCP}) \times (\text{entry length}(156)) )$   
 $+ ((\text{MAXNCPSZ}/2) \times (\text{entry length}(156)) )$   
 $+ ((\text{MAXNONCP}) \times (\text{2nd entry length } (40)) )$   
 $+ ((\text{MAXNCPSZ}/2) \times (\text{2nd entry length } (40)) ) )$

## Online Reporting

134K for each print report.

**In MVS/SP:** 678K for each summary/graph report.

1158K for each summary all report.

**In OS/390 and z/OS, and MVS/ESA:** 1245K for each summary/graph report.

2205K for each summary all report.

This storage space will be allocated above 16 MB in virtual storage, provided extended storage is available.

## RPL (Request Parameter List)

VTAM service used to manage NetSpy sessions:

$4024 \times (\text{MAXOPER} + \text{MAX\#NCP} + 16)$ .

## Session Control Blocks

$7076 \times (\text{MAXOPER} + \text{MAX\#NCP} + 6)$ .

MAXOPER is the maximum number of concurrent NetSpy operators.

## General Alerts

$(336 \times \text{AMAXENT}) + 21200 + (212 \times \text{the number of alerts held in global and user displays})$ .

The maximum number of alerts held in global and user displays is calculated by multiplying ALMAXE by (1 + the number of users with monitors requesting user alerts).

**In OS/390 and z/OS, and MVS/ESA running in ESA mode,** this storage space will be allocated above 16 bytes in virtual storage, provided extended storage is available.

## Help System

The amount of storage required depends on the language specified on the LANG statement:

LANGUAGE=EU: 675K

LANGUAGE=EJ: 675K

LANGUAGE=NA: 76K

In MVS/ESA and OS/390 and z/OS, this storage will be allocated above the 16 MB in virtual storage, provided extended storage is available.

## Number of Control Blocks Defined in the NCP

The LUDRPOOL and PUDRPOOL definition statements and the HSB (HSBPOOL) BUILD statement operand are specified in the NCP as follows:

Statement	Description
LUDRPOOL	Specifies the number of logical unit control blocks pooled for dynamically adding LUs to SDLC devices.
PUDRPOOL	Specifies the number of physical unit control blocks pooled for dynamically adding any SDLC devices to an NCP data link.

---

HSBPOOL	Specifies the number of half-session control blocks a gateway NCP makes available for cross-network sessions.
---------	---

---

**Note:** If you run NetSpy using all the defaults, which is usually more than adequate, a region size of 2000K should be enough. If you plan to use the online reporting facility, a region size of 4000K should be adequate. If you are collecting accounting records, this region size may need to be increased.

## CSA Storage Amounts

NetSpy uses the following amounts of CSA. Storage amounts are listed by NetSpy feature.

### Application Statistics

Amount of storage:<sup>2</sup>

- If running MVS/ESA in ESA mode: 504 x number of APPLs being monitored.
- If running any other MVS (OS/390 and z/OS) x number of APPLs being monitored.
- Plus, if running VTAM 3.2 or higher: 12 bytes x MAXAPPL

### Base Storage

10K

### Buffer Statistics

MAXJOBFF x 12 bytes

---

<sup>2</sup> For MVS/ESA releases, the application statistics, buffer trace blocks, exception trace buffers, and terminal statistics reside in NetSpy private storage.

## Buffer Trace Blocks

$\text{TRCBUFNO} \times (\text{blksize for trace files} + 4)^3$

**Notes:** This storage is allocated *only* while a buffer trace is active. See footnote on this page.

## Exception Trace Buffers

$(13 + \text{TRACELEN}) \times 5 + 29 \times \text{MAXTRACE}$ .

See footnote on this page.

## Monitoring Commands

$17 \times (\text{MAXTCMD} + \text{MAXFCMD} + \text{MAXTRINC} + \text{MAXTRALL})$

## SMF Type S Record Buffer

If writing type "S" records (SMF SESSION=YES): 328 bytes

## Terminal Statistics

Amount of storage<sup>4</sup> depends upon conditions:

- If running under MVS/ESA in ESA mode:  $140 \times \text{MAXLU}$
- If you are using global targets or transaction groups (TRANSGRP):  $108 \times \text{MAXLU}$
- If tracing is active and you are not using global targets:  $96 \times \text{MAXLU}$
- If tracing is inactive and you are not using global targets:  $92 \times \text{MAXLU}$

See footnote on this page.

---

<sup>3</sup> For MVS/ESA releases, the application statistics, buffer trace blocks, exception trace buffers, and terminal statistics reside in NetSpy private storage.

<sup>4</sup> For MVS/ESA releases, the application statistics, buffer trace blocks, exception trace buffers, and terminal statistics reside in NetSpy private storage.

## Virtual Route

$$(\text{MAXNOSA} \times 96) + (\text{MAXNOVR} \times 56)$$

For virtual route index blocks:

- If MAXNOSA is greater or equal to 625, then 42,816 bytes
- If MAXNOSA is less than 625, then the number of bytes equals  $(\text{MAXNOSA} + 44) \times 64$

## VTAM Tuning Statistics

Directly attached resources.

MAXCA CSA usage:  $\text{MAXCA} \times 76$  bytes

CINCLUDE CSA usage:  $\# \text{ NAMES} \times 10$  bytes

## Reducing Storage Requirements

You can reduce the requirements for CSA Common Storage by restricting the terminals NetSpy will monitor with the MAXLU statement or the MAXLU parameter on the APPL statement.

## Above 16 MB Line

NetSpy takes advantage of OS/390 and z/OS by taking all CSA from above 16 MB in virtual storage if you are running VTAM Version 3.

## Major Nodes Active

All VTAM application major nodes for the applications you wish to monitor must be active before NetSpy is started unless APPLNAME=NETNAME is specified.

## Multiple TCP/IP Stack Storage Amounts

The TCP/IP monitoring feature of NetSpy recommends that you run with a region size of 0M, otherwise various GETMAIN failures may result that could result in abends (such as 4093). Multiple TCP/IP stack support requires the following storage allocation.

### Allocation per stack being monitored

Total of 18,888 bytes.

These control blocks are getmained when a stack is added and freed, when the subtask associated with the stack shuts down, or when the stack is deleted.

### Allocation per TCP, UDP, or IF entry

This control block is getmained in 58,368 byte increments. This storage is never freed once allocated. Unused control blocks are available to be used by all stacks being monitored.

**Note:** Stack data storage is always allocated regardless of whether or not stack collection is set to Y (yes).

## Amount of Data Logged

NetSpy logs the following amount of data during each interval:

- 164 bytes for each LU monitored
- 340 bytes for each application specified in the initialization parameters
- 106 bytes for each NCP resource for which data is collected
- 288 bytes for each session when network accounting is collected. NetSpy will also log session start and end records when they occur.
- 204 bytes for each alert generated
- 68 bytes for each virtual route monitored
- 64 bytes for each VTAM buffer pool
- 77 bytes for each VTAM RTP for which data is collected
- 88 bytes for topology data
- 32 bytes for each MNPS application for which data is collected
- 24 bytes for each MNPS coupling facility structure

- 32 bytes for each recovery of MNPS application for which data is collected
- 64 bytes for directory services
- 179 bytes for each TCP/IP connection
- 192 bytes for STACK
- 76 per UDP connection
- 176 per IP interface

In addition, a 90-byte header starts each log record.

Therefore, the maximum number of bytes on disk that you will need for a typical day without network accounting is:

$$[(\text{MAXLU}) \times 164 + (\text{\#APPL}) \times 340 + (\text{sum of MAXCOLL in all NCPs being monitored}) \times 106 + (\text{MAXNOVR}) \times 68 + (\text{number of VTAM buffer pools}) \times 64] \times [\text{number of intervals per day}] + 204 \times (\text{number of alerts generated to a log in a given day}) + 90 \times (\text{number of log records written per day}) + (\text{\#TCP/IP connects}) \times 116 + (\text{\#RTPS}) \times 77 + (\text{Topology}=88) + [(\text{MNPS}) 32 \times (\text{\#APPL})] + (\text{\#MNPSCOUP}) \times 24 + (\text{\#MNPSREC}) \times 32 + (\text{Directory Services}=64) + (\text{TCP/IP STACK}=80).$$



# Answers to Common Questions

The following topics discuss some of the most frequently asked questions.

## How to Handle Abends

If you receive an abend error message (normally NSY0104), perform the following steps before calling technical support. Have a printed copy of the following diagnostic information available. Also see the section [How to Contact Technical Support](#).

1. Browse the NetSpy job log or the system log known as SYSLOG. An example of a NetSpy symptom dump that is typically found in either log is shown below.

```
STC04796 IEA9951 SYMPTOM DUMP OUTPUT
SYSTEM COMPLETION CODE=0C4 CPU=0000 ASID=008A
PSW AT TIME OF ERROR 078D2000 80028764 ILC 4 INTC11
ACTIVE LOAD MODULE=NSYMAIN ADDRESS=00006288 OFFSET=000224DC
DATA AT PSW 0002875E - 06205A10 A4285015 00001851
GPR 0-3 00000150 03763120 FFFFE05 00000150
GPR 4-7 006FBAD8 03763004 006E2FF8 00005FF8
GPR 8-11 006FF978 00116760 00028630 00029630
GPR 12-15 00008448 000289A0 40006456 00000000
END OF SYMPTOM DUMP
```

2. Using your symptom dump data, locate and write down the following three numbers:
  - a. The second full word of the PSW at the time of the error.  
(80028764 in our example data)
  - b. The contents of the 'ADDRESS=xxxxxxx' field.  
(00006288 in our example data)
  - c. The contents of GPR '10' (Base Register R10)  
(00028630 in our example data)

- Using the above numbers from your data, complete the following calculations. Calculations are in hexadecimal format.

**Offset into module that abended:**

PSW - R10 = offset  
(Example: 28764 - 28630 = +134 offset)

**Note:** The high-order bit of the PSW is the addressing mode and should be ignored in this calculation.

**Location of module that abended:**

R10 - ADDR = location  
(Example: 28630 - 6288 = 223A8)

- Call technical support and have ready the two calculations from Step 3 above.

## Authorizing NetSpy to Run at Your Site

When your site receives a license for NetSpy, Computer Associates provides a CA LMP Key Certificate that identifies a single CPU that is authorized to run NetSpy. The certificate contains a CA LMP execution key that you must define to the CAIRIM parameters. You will need to obtain a new CA LMP Key Certificate whenever you install NetSpy on a new CPU. Call the CA TLC (Total License Care) number published in the CA Product Support Directory.

## Sharing Log Files

Each NetSpy application in your system has its own logs to which it writes log records. Do not attempt to have multiple NetSpys write to the same physical logs. Sharing logs between NetSpys can result in contention problems and corrupted data.

However, you can coordinate data from multiple logs into central logs for reporting. Refer to Log Files in the chapter entitled “Displaying Historical Data” for information on how to request data from multiple logs.

## Updating the *dsnpref.NYvvv.NYLOAD* Data Set

Whenever you receive a new NetSpy release, you should always download the *dsnpref.NYvvv.NYLOAD* data set from the tape to DASD. Never reuse the *dsnpref.NYvvv.NYLOAD* data set from a previous release; doing so may trigger an abend due to inadequate space allotment for the new release. For complete instructions on loading the data sets, refer to the NetSpy *Getting Started* guide.

## Mapping Line and Cluster Data to NTRI and X.25 Resources

The following scenarios show what NetSpy displays and writes to log records based on how you configure the parameters in the STARTPRM file for mapping line and cluster data.

**Note:** All definitions refer to the DEFINE statements in the STARTPRM file.

### Scenario #1: NCP and No Switched Major Node Defined

If you define:	You will see:
<i>ncpname</i> MON=NO	<p><b>On the Node Monitoring Status Screen:</b> Switched LU name will not be displayed</p> <p><b>On the Terminal Response Time Analysis Screen:</b> Switched LU name No Line/Cluster mapping</p> <p><b>In the Type T and U Log Record Data:</b> Switched LU name No Line/Cluster mapping</p>

### Scenario #2: NCP and Switched Major Node Defined Last

---

<b>If you define:</b>	<b>You will see:</b>
<i>ncpname</i> MON=NO Switched major node	<b>On the Node Monitoring Status Screen:</b> Switched LU name displayed under the switched major node and switched PU  <b>On the Terminal Response Time Analysis Screen:</b> Switched LU name Line name = switched major node name Cluster = switched PU  <b>In the Type T and U Log Record Data:</b> Switched LU name Line name = switched major node name Cluster = switched PU

---

### Scenario #3: NCP and Switched Major Node Defined Last

---

<b>If you define:</b>	<b>You will see:</b>
<i>ncpname</i> MON=YES Switched major node	<b>On the Node Monitoring Status Screen:</b> Switched LU name displayed under the switched major node and switched PU  <b>On the Terminal Response Time Analysis Screen:</b> Switched LU name Line name = switched major node name Cluster = switched PU  <b>In the Type T and U Log Record Data:</b> Switched luname Linename = switched major node name Cluster = switched PU

---

**Scenario #4: NCP and Switched Major Node Defined First**

<b>If you define:</b>	<b>You will see:</b>
Switched major node <i>ncpname</i> MON=NO	<p><b>On the Node Monitoring Status Screen:</b> Switched LU name displayed under the switched major node and switched PU</p> <p><b>On the Terminal Response Time Analysis Screen:</b> Switched LU name No Line/Cluster mapping</p> <p><b>In the Type T and U Log Record Data:</b> Switched LU name No Line/Cluster mapping</p>

**Scenario #5: NCP having 'NPA=(YES,DR)' and Switched Major Node Defined First**

<b>If you define:</b>	<b>You will see:</b>
Switched major node <i>ncpname</i> MON=YES	<p><b>On the Node Monitoring Status Screen:</b> Switched LU name displayed under the PLINK, LLINK, LLINK PU and switched PU</p> <p><b>On Terminal Response Time Analysis Screen:</b> Switched LU name Line name = LLINK Cluster = Switched PU</p> <p><b>In the Type T and U Log Record Data:</b> Switched LU name Line name = LLINK Cluster = Switched PU</p>

**Scenario #6: NCP having 'NPA=(YES)' and Switched Major Node Defined First**

<b>If you define:</b>	<b>You will see:</b>
Switched major node <i>ncpname</i> MON=YES	<p><b>On the Node Monitoring Status Screen:</b> Switched LU name displayed under the switched major node and switched PU</p> <p><b>On the Terminal Response Time Analysis Screen:</b> Switched LU name No Line/Cluster mapping</p> <p><b>In the Type T and U Log Record Data:</b> Switched LU name No Line/Cluster mapping</p>

## Using the Enhanced Application Monitoring Feature

The Enhanced Application Monitoring feature lets NetSpy monitor sessions where the application is the SLU as well as the PLU.

For this feature to work, you must have the following:

- VTAM 3.2 or above
- The APPLNAME=NETNAME statement coded in the INITPRM
- At least one of the session partners must be a VTAM application residing in the same domain as NetSpy

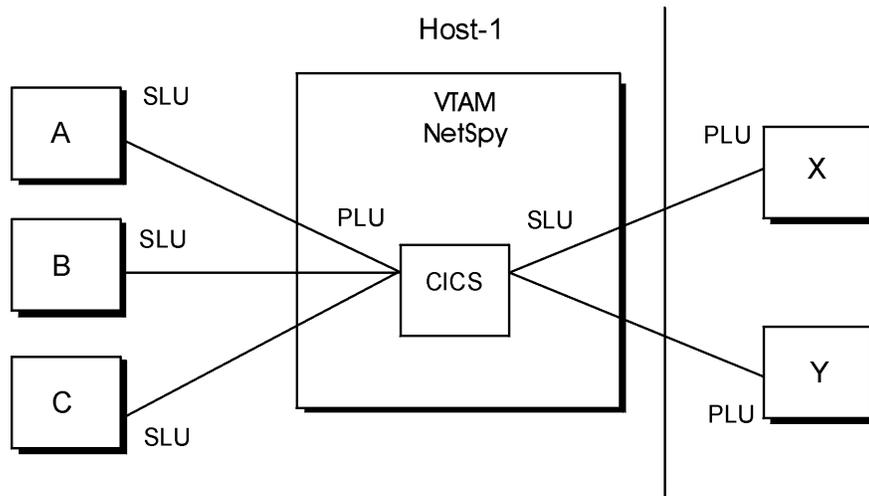
### How PLUs and SLUs Are Displayed

If the PLU is defined to NetSpy on an APPL statement in the INITPRM member, then the session is monitored under that application.

If the PLU is *not* defined on an APPL statement, and the SLU is defined on an APPL statement *and* APLTOAPL=ENHANCED is coded or allowed to default in INITPRM, then the session will be reported under the SLU name defined on an APPL statement.

### Scenarios

The following scenarios show what is displayed in online screens and historical log records based on how you configure the APLTOAPL and APPL parameters in INITPRM. Each scenario refers to what is displayed on the Terminal Traffic and Response Time screen. Refer to the illustration below when reading the scenarios. In the illustration, A, B, and C are SLUs, and X and Y are PLUs. Resources A, B, C, X, and Y can be either applications or PC-type devices running applications and acting as a PLU.



**Scenario #1: APLTOAPL=NORMAL**

<b>If you define:</b>	APPL=CICS
<b>You will see:</b>	A session entry under the CICS application heading for resources A, B, and C.

**Scenario #2: APLTOAPL=NORMAL**

<b>If you define:</b>	APPL=CICS APPL=X APPL=Y
<b>You will see:</b>	All of the following: <ul style="list-style-type: none"> <li>■ A session entry under the CICS application heading for resources A, B, and C.</li> <li>■ A session entry for CICS under each of the application headings for X and Y.</li> </ul>

**Scenario #3: APLTOAPL=ENHANCED**

<b>If you define:</b>	APPL=CICS
<b>You will see:</b>	A session entry under the CICS application heading for resources A, B, C, X, and Y.

**Scenario #4: APLTOAPL=ENHANCED**

<b>If you define:</b>	APPL=CICS APPL=X APPL=Y
<b>You will see:</b>	A session entry under the CICS application heading for resources A, B, and C.  'CICS' under each of the application headings for X and Y.

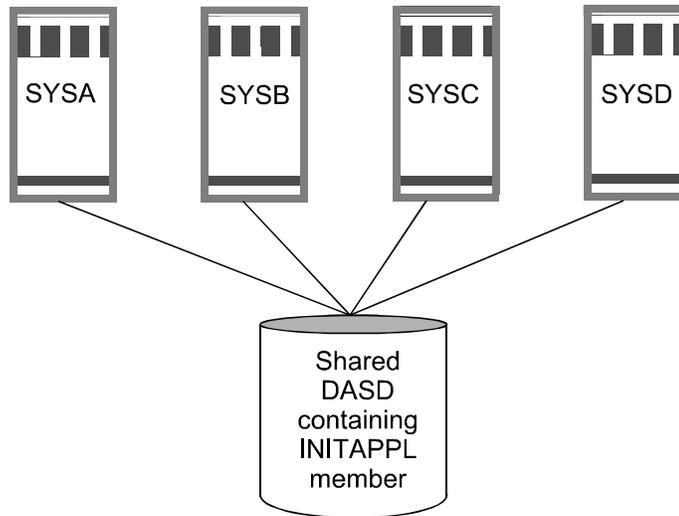
**Scenario #5: APLTOAPL=NORMAL or APLTOAPL=ENHANCED**

<b>If you define:</b>	APPL=X APPL=Y
<b>You will see:</b>	A session entry for CICS under the application headings for X and Y only. NetSpy would not report any information for resources A, B, and C.

## Configuring NetSpy in a Sysplex Environment

This section describes how you can configure NetSpy in a sysplex operating environment.

The illustration below shows a sample sysplex network configuration consisting of four independent hosts. It is recommended that all hosts share a common DASD volume where the NetSpy control and load libraries reside.



Each system in the sample scenario has a unique INITPRM member, with a secondary concatenation of a common member (in this example, INITAPPL) made up of NetSpy APPL= definitions. The common member contains all VTAM applications that you want NetSpy to monitor.

Shared DASD offers these benefits:

- You need to update only one PROCLIB to customize the NetSpy started task JCL
- You need to update only one LOADLIB to apply maintenance
- You can place APPL statements for all NetSpys in one member

### Sample JCL Statements

Sample NetSpy PROC statements for the INITPRM DD card would look like this:

```
//INITPRM DD DISP=SHR,DSN=dsnpref.NYvvv.CNTL(INITSYSx) <== x is the SYSID suffix
//          DD DISP=SHR,DSN=dsnpref.NYvvv.CNTL(INITAPPL) <== Common APPL
                                                    definition member
```

## How to Contact Technical Support

Before contacting technical support, please try to resolve your problem by reading the manuals that are provided with the software and by using the NetSpy help system.

Refer to the section [How to Handle Abends](#) in this chapter for instructions on solving common NetSpy problems, and for additional information you should provide when calling about a particular problem.

### Information You Can Provide

Please have the following information ready when you contact technical support:

- Product version number shown on the main NetSpy menu screen.
- The type of computer hardware you are running NetSpy on.
- The version number of the operating system, VTAM, or NCP.
- The message number and exact wording of any error messages you may have received online, in the NetSpy job log, or on the system console.
- What you were doing when the problem occurred.
- How you tried to solve the problem.

### Ways to Contact

See the appendix entitled “Contacting Technical Support” in this manual for a full description of using Computer Associates Technical Support services, including the technical support services available on the World Wide Web.

# Contacting Technical Support

---

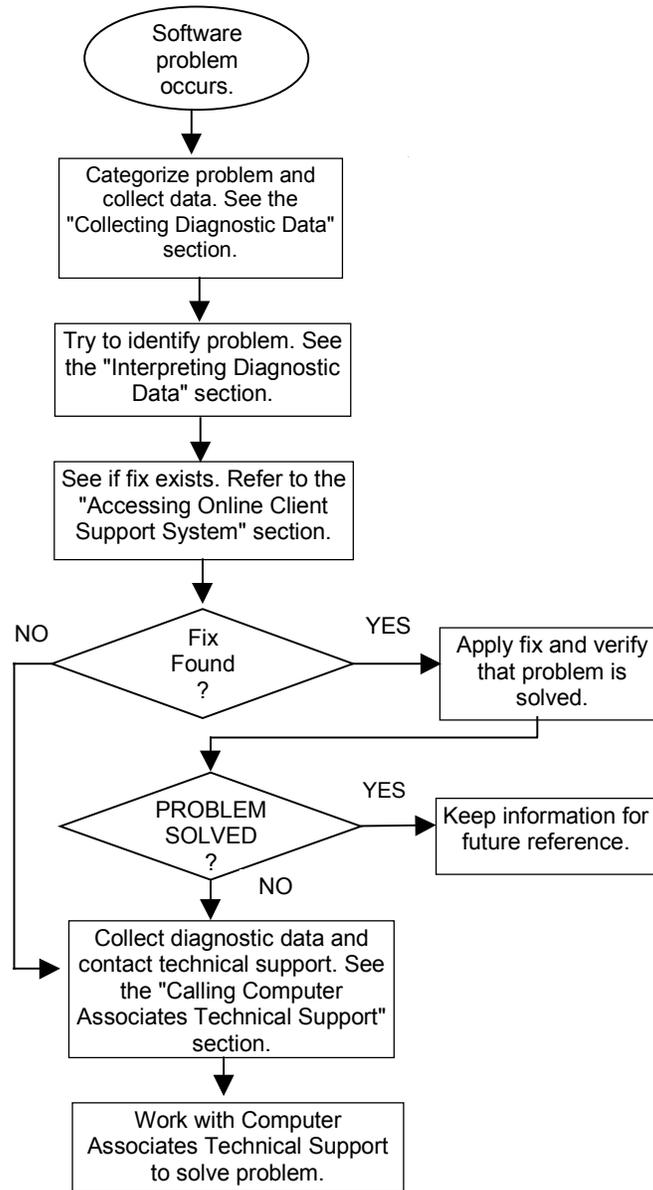
## Overview

This chapter contains information about:

- Identifying and resolving problems
- Contacting Computer Associates Technical Support
- Receiving ongoing product releases and maintenance
- Requesting product enhancements

## Diagnostic Procedures

Refer to the flowchart below for a summary of the procedures you should follow if you have a problem with a Computer Associates software product. Each of these procedures is detailed on the following pages.



## Collecting Diagnostic Data

The following information is helpful in diagnosing problems that might occur:

- Control statements used to activate your product
- JCL used to install or activate your product
- Relevant system log or console listings
- Relevant system dumps or product dumps
- List of other IBM or third-party products that might be involved
- Manufacturer, model number, and capacity of your hardware
- Numbers and text of IBM or CA error messages associated with the problem
- Names of panels where the problem occurs
- Listings of all fixes applied to all relevant software, including:
  - The dates the fixes were applied
  - Fix numbers
  - Names of components to which fixes were applied
- Short description of problems

## Interpreting Diagnostic Data

When you have collected the specified diagnostic data, write down your answers to the following questions:

1. What was the sequence of events prior to the error condition?
2. What were the circumstances when the problem occurred and what action did you take?
3. Has this situation occurred before? What was different then?
4. Did the problem occur after a particular PTF was applied or after a new release of the software was installed?
5. Have you recently installed a new release of the operating system?
6. Has the hardware configuration (tape drives, disk drives, and so forth) changed?

From your response to these questions and the diagnostic data, try to identify the cause and resolve the problem.

## Accessing the Online Client Support System

StarTCC, the web-based portion of CA-TCC (CA-Total Client Care), gives you real time, interactive access to Computer Associates product support information through the Internet. Using StarTCC, you can:

- Open new issues
- Browse or update your existing issues
- Perform keyword searches
- Download solutions, service packs, and important notices regarding Computer Associates products, maintenance, and documentation

### Requirements for Using StarTCC

The following are the requirements to use StarTCC:

- You must be a CA client with a current maintenance agreement.
- You must register through the CA Internet site.
- You must access the Internet with a browser that supports the HTML specification 2.0 or higher, such as Netscape Navigator 2.0 or higher or Microsoft Internet Explorer 3.0 or higher. (You can download one of these browsers from the CA Technical Support page.)

Browsers that meet the HTML requirement support the following functions, which are required for StarTCC:

- Secure sockets layer (SSL) to encrypt your transaction traffic
- Encrypted data records (known as COOKIES)
- HTML tables

### StarTCC Security

StarTCC runs as a secured server (SSL). You may need to configure your browser to enable SSL. Guidelines for doing this are provided on the CA Technical Support page.

## Accessing StarTCC

To access StarTCC, access <http://esupport.ca.com> or click the Support button on the CA home page and follow the links for StarTCC.

If you are a first time user, you must register before you can access StarTCC online. Select the registration option to identify yourself to StarTCC. There are prompts for all required information, including your name, site ID, CA-StarTrak PIN, company name, e-mail address, postal address, and desired password for accessing StarTCC.

**Note:** If you do not have a CA-StarTrak PIN, StarTCC provides one for you when you register.

Select the access option to begin using StarTCC. When prompted, enter your user ID and password.

## Accessing the Product Support Directory Online

The Computer Associates Product Support Directory lists each CA product and the telephone number to call for primary support for that product. To access the Product Support Directory online, click the Support button on the CA home page. Follow the links.

## CA-TLC: Total License Care

Many CA software solutions use license keys or authorization codes to validate your hardware configuration. If you need assistance obtaining a license key or authorization code, contact the CA-TLC: Total License Care group at 1-800-338-6720.

## Calling Computer Associates Technical Support

Computer Associates provides telephone support for all its products.

If you are in North America, refer to the *Product Support Directory* for the specific CA Technical Support phone number for each product. Outside North America, call your local Computer Associates Support Center during normal business hours.

Emergency phone numbers are also available for after-hours technical support. After hours calls should be limited to severity 1 problems.

**Note:** Only your local Computer Associates Support Center can provide native language assistance. Please use English when contacting any North American center.

If you are unable to resolve the problem, please have the following information ready before contacting Computer Associates Technical Support:

- All the diagnostic information described in Collecting Diagnostic Data.
- Product name, release number, operating system and service pack.
- Product name and release number of any other software you suspect is involved.
- Release level of the operating system.
- Your name, telephone number, and extension (if any).
- Your company name.
- Your site ID.
- A severity code. This is a number (from 1 to 4) that you assign to the problem. Use the following to determine the severity of the problem:
  1. A “system down” or inoperative condition
  2. A suspected high-impact condition associated with the product
  3. A question concerning product performance or an intermittent low-impact condition associated with the product
  4. A question concerning general product utilization or implementation

## Product Releases and Maintenance

Clients are requested to operate only under currently supported releases of the product.

Clients with current maintenance agreements also receive ongoing maintenance. When a new release of the system is available, a notice is sent to all current clients.

## Requesting Enhancements

Computer Associates welcomes your suggestions for product enhancements. All suggestions are considered and acknowledged. You can use either of two methods to request enhancements:

- Access StarTCC from the CA web site to open an issue for the enhancement request. For details, see [Accessing the Online Client Support System](#) in this chapter.
- Contact your account manager or a technical support representative who will initiate a Demand Analysis Request (DAR) for you.



# Index

## 3

---

3746 Nways Model 950 controller. *See* Nways Model 950 controller

## A

---

abends, NetSpy, B-1  
ACCESS parameter, 1-55  
accounting, 6-1, 6-2  
    gateway, 1-5, 2-11  
    session, 1-5, 2-11  
    type C records, 10-8  
ACCSSRTM statement, 1-4  
ACCTING statement, 1-5  
ALDESC statement, 1-5  
ALERTPRM member, 3-1  
alerts, 3-1  
ALIAS parameter, 1-9  
ALMAXE statement, 1-6  
ALROUT statement, 1-6  
ALTBITVL statement, 1-7  
ALWRITE statement, 1-7  
AMAXENT statement, 1-7  
APLTOAPL statement, 1-15  
APPL statement, 1-8  
application log record, 10-5  
APPLNAME statement, 1-14

APPN monitor  
    installing, 14-1  
    log records, 10-12, 10-39, 10-40  
AUDITCLS statement, 1-15  
AUDITDST statement, 1-15  
authorization code, B-2

## B

---

BASEITVL statement, 1-16  
BTH parameter, 2-12  
BUILD definition statement, 6-1

## C

---

CA-ACF2, 5-1, 5-3, 5-4  
CA-Datacom, 4-1, 4-2  
CA-Datacom Server, 4-2  
CAICCI, 4-2  
CAIENF, 4-2  
CAIRIM, 4-2  
CA-Teleview, 8-1  
CA-Teleview releases, 8-3  
CA-TLC (Total License Care), C-5  
CA-Top Secret, 5-1, 5-3  
CA-TPX, 8-1  
CINCLUDE statement, 1-16  
CL/Supersession, 8-1

---

CNFGITVL statement, 1-17  
COLLECT POLLSTAT statement, 2-6  
COLLECT statement, 2-2  
comment delimiter, 1-2  
CONNECT statement, 2-7  
CONSINTF statement, 1-17  
converting  
    Database records to SMF format, 13-1  
    log records to Database format, 13-2  
    log records to NPM type 28, 12-1  
    log records to SMF type 38, 11-1  
cross-NetSpy communication. *See* NetSpy-to-NetSpy communication  
CSA requirements, A-7  
customizing parameters online, 2-1

## D

---

Database, 2-4  
    allocating, 4-3  
Database utilities  
    NSYDBCV, 13-1  
    NSYDBLD, 13-2  
    NSYDCP, 13-2  
Datacom. *See* Database  
DBSTART statement, 1-18  
DBSTOP statement, 1-18  
DEFINE statement, 2-8  
diagnostics  
    enhanced application monitoring, B-6  
    handling abends, B-1  
    JCL updates, B-3  
    sharing log files, B-3  
    updating data sets, B-3  
DNSMF statement, 1-19  
dynamic reconfiguration, 6-1

## E

---

EOT parameter, 1-10  
Ethernet Adapter log records, 10-32  
exception trace record layout, 10-51

## F

---

FINCLUDE/FEXCLUDE statement, 1-19  
FORCEDR parameter, 1-56  
FORCEDR statement, 1-20  
Frame Relay log records, 10-33

## G

---

gateway accounting, 1-5, 2-11, 6-2  
general alert log records, 10-47  
generic name, 1-2  
    using in NCP definition, 2-8  
GMAXENT statement, 1-21  
GWESAC parameter, 6-2

## H

---

HCUTOFF statement, 1-21  
HOSTID statement, 1-22  
HPR log records, 10-22  
HPRDATA statement, 1-22  
HSBPOOL BUILD statement operand, A-6

---

## I

---

IGNRLOGN statement, 1-22

initialization parameters

ACCESS, 1-55  
ACCSRTM, 1-4  
ACCTING, 1-5  
ALDESC, 1-5  
ALIAS, 1-9  
ALMAXE, 1-6  
ALROUT, 1-6  
ALTBITVL, 1-7  
ALWRITE, 1-7  
AMAXENT, 1-7  
APLTOAPL, 1-15  
APPL, 1-8  
APPLNAME, 1-14  
AUDITCLS, 1-15  
AUDITDST, 1-15  
BASEITVL, 1-16  
CINCLUDE, 1-16  
CNFGITVL, 1-17  
CONSINTF, 1-17  
DBSTART, 1-18  
DBSTOP, 1-18  
DNSMF, 1-19  
EOT, 1-10  
FINCLUDE/FEXCLUDE, 1-19  
FORCEDR, 1-20, 1-56  
GMAXENT, 1-21  
HCUTOFF, 1-21  
HOSTID, 1-22  
HPRDATA, 1-22  
IGNRLOGN, 1-22  
INTERVAL, 1-23  
LANGUAGE, 1-23  
LOGDUMP, 1-24  
LOGSTART, 1-24  
LOGSTOP, 1-25  
LOGTYPE, 1-25  
LOSTDATA, 1-26  
LU62RESP, 1-26  
LUNAME, 1-55  
MAX#NCP, 1-27  
MAX#NRPT, 1-28  
MAXAPPL, 1-28  
MAXCA, 1-29  
MAXCOLL, 6-3  
MAXFCMD, 1-29  
MAXJOBBJ, 1-30  
MAXLU, 1-30  
MAXNCPSZ, 1-31  
MAXNOSA, 1-32  
MAXNOVR, 1-32  
MAXOPER, 1-33  
MAXTCMD, 1-34  
MAXTRACE, 1-34  
MAXTRALL, 1-35  
MAXTRINC, 1-35  
NCPRETRY, 1-36  
NCUTOFF, 1-36  
NETRSP, 1-37  
NEUPERF, 1-37  
NSYNAME, 1-38  
NSYXNAME, 1-39  
NTARGETS, 1-40  
NULLTREC, 1-41  
OPTMODE, 1-41  
PMI, 1-43  
RIFNORM, 1-44  
SECURE, 1-44, 5-2  
SESSION, 1-45  
SMF, 1-45  
SMFSTART, 1-46  
SMFSTOP, 1-46  
SNAMDATA, 1-47  
SNMPAGNT, 1-48  
SNMPHOST, 1-50  
STOP, 1-52  
SYNC, 1-53  
TARGET, 1-8  
TARGETS, 1-53  
TCPIPMON, 1-54  
TELNETLU, 1-55  
TINCLUDE/TEXCLUDE, 1-57  
TNMON, 1-13  
TRACE, 1-58  
TRACEALL, 1-12, 1-58  
TRACEEXC, 1-59  
TRACEHST, 1-60  
TRACEINC, 1-60  
TRACELN, 1-61  
TRACENET, 1-61  
TRACEUSR, 1-13, 1-62  
TRANSGRP, 1-62  
TRCBUFNO, 1-63  
TRCSTART, 1-63  
TRCSTOP, 1-64  
TRLENGTH, 1-12, 1-58  
TRSTARTT, 1-13, 1-59  
TRSTOPT, 1-13, 1-59  
TYPEU, 1-45  
USRIDUPD, 1-64  
UTARGETS, 1-65  
VTAMINTF, 1-66

---

INITPRM member/file, 1-1

Interface entry  
log records, 10-14

INTERVAL statement, 1-23

## L

---

LANGUAGE statement, 1-23

line, controller, terminal log records, 10-23

LMP code, B-2

Log, 2-4

log record layouts

- generic type N, 10-19
- SMF header, 10-2
- type A, 10-5
- type B, 10-7
- type C, 10-8
- type E (APPN Directory Services), 10-12
- type E (MNPS Application Recovery), 10-13
- type F (MNPS Coupling Facility Structure Data), 10-13
- type G (UDP), 10-13
- type H (Interface), 10-14
- type I (TCP), 10-15
- type J (stack), 10-16
- type N (Ethernet Adapter), 10-32
- type N (Frame Relay), 10-33
- type N (HPR), 10-22
- type N (line, controller, terminal), 10-23
- type N (NCP control block), 10-35
- type N (NCP major node), 10-25
- type N (NTRI), 10-28
- type N (TIC3), 10-30
- type N (transmission priority), 10-38
- type N (X.25 NPSI), 10-26
- type P (APPN topology), 10-39
- type R (VTAM RTP), 10-40
- type S (terminal session), 10-41
- type T and U (terminal), 10-43
- type V (virtual route), 10-45
- type X (general alert), 10-47

log record types, 10-1

LOGDUMP statement, 1-24

logging NetSpy data, 2-4

LOGSTART statement, 1-24

LOGSTOP statement, 1-25

LOGTYPE statement, 1-25

LOSTDATA statement, 1-26

LU62RESP statement, 1-26

LUDRPOOL definition statement, A-6

LUNAME parameter, 1-55

## M

---

MAX#NCP statement, 1-27

MAX#NRPT statement, 1-28

MAXAPPL statement, 1-28

MAXCA statement, 1-29

MAXCOLL parameter, 6-3

MAXFCMD statement, 1-29

MAXJOBBJ statement, 1-30

MAXLU statement, 1-30

MAXNCPSZ statement, 1-31

MAXNOSA statement, 1-32

MAXNOVR statement, 1-32

MAXOPER statement, 1-33

MAXTCMD statement, 1-34

MAXTRACE statement, 1-34

MAXTRALL statement, 1-35

MAXTRINC statement, 1-35

MNPS monitor  
log records, 10-13

MON parameter, 2-9

MONITOR statements, 3-2

multiple NetSpys  
collecting data from, 2-2

---

## N

---

N28CONV program, 12-1  
parameters, 12-2

NCP  
control block log records, 10-35  
defining to NetSpy, 2-8  
generation, 6-1  
interface  
troubleshooting, 6-4  
major node log records, 10-25  
parameter, 2-12  
regeneration of, 2-8

NCPRETRY statement, 1-36

NCUTOFF statement, 1-36

NETACCT statement, 2-11

NetMaster, 8-1

NET-PASS, 8-1

NETRSP statement, 1-37

NETSPY parameter, 2-4, 2-6, 2-7

NetSpy-to-NetSpy communication, 2-2  
starting, 2-8

NetView interface  
enabling, 9-1  
return codes, 9-3

network accounting, 1-5, 2-11

NEUPERF  
parameter, 7-1

NEUPERF statement, 1-37

NODE parameter, 2-6

NPA definition statements, 6-2, 6-3

NPALU parameter, 2-10

NSNYHIST  
control statements, 7-3

NSYCONV program, 11-1  
parameters, 11-2

NSYBCV utility, 13-1

NSYBLD utility, 13-2

NSYDCP utility, 13-2

NSYNAME statement, 1-38

NSYXNAME statement, 1-39

NTARGETS statement, 1-40

NTRI log records, 10-28

NULLTREC statement, 1-41

Nways Model 950 controller, 2-10

NWAYS parameter, 2-8, 2-10

## O

---

online tailoring of parameters, 2-1

OPTMODE statement, 1-41

## P

---

PIUDIST parameter, 2-13

PMI statement, 1-43

PROC, 4-4

PTH parameter, 2-13

PUDRPOOL definition statement, A-6

purging the Database, 13-2

## R

---

RACF, 5-1, 5-3

resource types, 2-2

response time  
calculating, 2-6

RETRY parameter, 2-10

RIFNORM statement, 1-44

---

## S

---

SCOPE parameter, 2-2, 2-14

SECURE parameter, 5-2

SECURE statement, 1-44

security interface, 5-1

- files, 5-2
- installing, 5-2

SESSACC parameter, 6-1

session accounting, 1-5, 2-11, 6-1

session manager interface

- installing, 8-1
- monitoring functions, 8-1
- testing, 8-3

session managers

- supported, 8-1

SESSION parameter, 1-45

SMF record header, 10-2

SMF record types, 10-1

SMF statement, 1-45

SMFSTART statement, 1-46

SMFSTOP statement, 1-46

SNA Manager Option. *See* Unicenter SNA Manager Option

SNAMDATA statement(for Unicenter SNA Manager Options only, 1-47

SNMP, 4-2

SNMPAGNT statement, 1-48

SNMPHOST statement, 1-50

- OMVS security segment, 1-50

SSMF statement, 2-14

STARTPRM member/file, 2-1

STARTT and STOPT parameters, 2-4

startup parameters

- COLLECT, 2-2
- COLLECT POLLSTAT, 2-6
- CONNECT, 2-7
- DEFINE, 2-8
- NETACCT, 2-11
- SSMF, 2-14

STOP statement, 1-52

storage requirements, A-7

support, contacting, B-10

SYNC statement, 1-53

---

## T

---

TARGET parameter, 1-8

TARGETS statement, 1-53

TCP connection

- log records, 10-15

TCP/IP, 4-2

TCP/IP monitor, 1-54

TCPIPMON statement, 1-54

technical support, contacting, B-10

TELNETLU statement, 1-55

terminal log records, 10-43

terminal prefix, 1-2

terminal session log records, 10-41

TIC3 log records, 10-30

TINCLUDE/TEXCLUDE statement, 1-57

TNMON parameter, 1-13

trace record layout, 10-51

TRACE statement, 1-58

TRACEALL parameter, 1-12

TRACEALL statement, 1-58

TRACEEXC statement, 1-59

TRACEHSTstatement, 1-60

TRACEINC statement, 1-60

TRACELen statement, 1-61

TRACENET statement, 1-61

TRACEUSR parameter, 1-13

TRACEUSR statement, 1-62

transaction-all trace records, 10-51

TRANSGRP statement, 1-62

---

transmission priority log records, 10-38

TRCBUFNO statement, 1-63

TRCSTART statement, 1-63

TRCSTOP statement, 1-64

TRLENGTH parameter, 1-12, 1-58

troubleshooting, C-1

TRSTARTT parameter, 1-13, 1-59

TRSTOPT parameter, 1-13, 1-59

type 28 records, 12-1

type 38 records, 11-1

TYPEU parameter, 1-45

## U

---

UDP connection  
log records, 10-13

Unicenter, 3-10, 4-1  
Framework for OS/390, 4-2  
Interface, parameters for, 4-7  
SNA Manager Option, 1-47, 4-1

USRIDUPD statement, 1-64

UTARGETS statement, 1-65

## V

---

virtual route log records, 10-45

virtual storage requirements, A-1

VTAM buffer statistics log record, 10-7

VTAMINTF statement, 1-66

## X

---

X.25 NPSI log records, 10-26