z/OS Communications Server

OA49911 - 3270 Intrusion Detection Services (part 2)

Version 2 Release 2

Note:
Links to related publications are from original documents and might not work. The links to publications are included for reference purposes only.

Contents

Tables

Chapter 1. IP Programmer's Guide and Reference

C/C++ applications

For C/C++ applications, the following header files provide the SMF record mappings:

ezasmf.h
This header file provides mappings for most of the SMF records.

ezbnmmpc.h
This header file provides the mappings for the individual sections of profile data in the SMF 119 TCP/IP profile SMF event record (subtype 4).

Both header files are installed in the SEZANMAC MVS™ data set and in the /usr/include file system directory.

SMF 119 record subtypes

TCP/IP collects SMF information about certain Telnet, FTP, TCP/IP stack, IKE daemon, CSSMTP, or VTAM 3270 Intrusion Detection activity. These records can be generated by the TCP/IP stack, the FTP and Telnet clients and server, the IKE daemon, the CSSMTP client, or VTAM. You can control the collection of these records by using the SMFCONFIG statements in PROFILE.TCPIP, or by using statements in the various application's configuration files. For more information about those statements, see z/OS Communications Server: IP Configuration Reference.

All the records described in this topic are written using record type 119 (X'77'), and standard subtype values, at offset 22 (X'16') in SMF record header, are used to uniquely identify the type of record being collected. Table 1 correlates the subtype information to the type of record being produced.

Table 1. SMF 119 record subtype information and record type

Record subtype	Description	TCP/IP component event	Reason
1(X'1')	TCP connection initiation record (subtype 1)	TCP	Event
2(X'2')	TCP connection termination record (subtype 2)	TCP	Event
3(X'3')	FTP client transfer completion record (subtype 3)	FTPC	Event
4(X'4')	TCP/IP profile event record (subtype 4)	STACK	Event
5(X'5')	TCP/IP statistics record (subtype 5)	STACK	Interval
6(X'6')	Interface statistics record (subtype 6)	IP	Interval
7(X'7')	Server port statistics record (subtype 7)	STACK	Interval
8(X'8')	TCP/IP stack start/stop record (subtype 8)	TCP	Event
9	Reserved		
10(X'A')	UDP socket close record (subtype 10)	UDP	Event
11–19	Reserved		

Table 1. SMF 119 record subtype information and record type (continued)

Record subtype	Description	TCP/IP component event	Reason
20(X'14')	TN3270E Telnet server SNA session initiation record (subtype 20)	TN3270S	Event
21(X'15')	TN3270E Telnet server SNA session termination record (subtype 21)	TN3270S	Event
22(X'16')	TSO Telnet client connection initiation record (subtype 22)	TN3270C	Event
23(X'17')	TSO Telnet client connection termination record (subtype 23)	TN3270C	Event
24–31	Reserved		
32(X'20')	DVIPA status change record (subtype 32)	STACK	Event
33(X'21')	DVIPA removed record (subtype 33)	STACK	Event
34(X'22')	DVIPA target added record (subtype 34)	STACK	Event
35(X'23')	DVIPA target removed record (subtype 35)	STACK	Event
36(X'24')	DVIPA target server started record (subtype 36)	STACK	Event
37(X'25')	DVIPA target server ended record (subtype 37)	STACK	Event
38–40	Reserved		
41(X'29')	SMC-R link group statistics record (subtype 41)	SMCR	Interval
42(X'2A')	SMC-R link state start record (subtype 42)	SMCR	Event
43(X'2B')	SMC-R link state end record (subtype 43)	SMCR	Event
44(X'2C')	RDMA network interface card (RNIC) interface statistics record (subtype 44)	SMCR	Interval
45–47	Reserved		
48(X'30')	CSSMTP configuration record (CONFIG subtype 48)	CSSMTP	Event
49(X'31')	CSSMTP connection record (CONNECT subtype 49)	CSSMTP	Event
50(X'32')	CSSMTP mail record (MAIL subtype 50)	CSSMTP	Event
51(X'33')	CSSMTP spool file record (SPOOL subtype 51)	CSSMTP	Event
52(X'34')	CSSMTP statistical record (STATS subtype 52)	CSSMTP	Interval
53–69	Reserved		
70(X'46')	FTP server transfer completion record (subtype 70)	FTPS	Event
71(X'47')	FTP daemon configuration record (subtype 71)	FTPD	Event
72(X'48')	FTP server logon failure record (subtype 72)	FTPS	Event
73(X'49')	IPSec IKE tunnel activation and refresh record (subtype 73)	IKE	Event

Table 1. SMF 119 record subtype information and record type (continued)

Record subtype	Description	TCP/IP component event	Reason
74(X'4A')	IPSec IKE tunnel deactivation and expire record (subtype 74)	IKE	Event
75(X'4B')	IPSec dynamic tunnel activation and refresh record (subtype 75)	IKE	Event
76(X'4C')	IPSec dynamic tunnel deactivation record (subtype 76)	IKE	Event
77(X'4D')	IPSec dynamic tunnel added record (subtype 77)	STACK	Event
78(X'4E')	IPSec dynamic tunnel removed record (subtype 78)	STACK	Event
79(X'4F')	IPSec manual tunnel activation record (subtype 79)	STACK	Event
80(X'50')	IPSec manual tunnel deactivation record (subtype 80)	STACK	Event
80(X'50')	IPSec manual tunnel deactivation record (subtype 80)	STACK	Event
81(X'51')	"VTAM 3270 Intrusion Detection Services event record (subtype 81)" on page 5	IDS3270	Event
82–93	Reserved		
94(X'5E')–98(X'62')	OpenSSH		
99-255	Reserved		

Notes:

1. The TCP/IP component indicated is the one reported in the TCP/IP identification section for each record (see the following sections).
2. The Reason indicated determines whether each record is an event record (it is flagged with a reason code of X'08'; in the TCP/IP identification section) or an interval record (it is flagged with one of the six interval reason codes in the TCP/IP identification section).
3. The OpenSSH element of z/OS® also creates SMF 119 records with subtypes of 94 through 98. For a description of these records, see z/OS OpenSSH User's Guide.
4. VTAM also creates SMF 119 records with a subtype of 81.

Common TCP/IP identification section

The Common TCP/IP identification section is present in every SMF Type 119 record. This section is to identify the system and the TCP/IP stack or other address space responsible for producing the record. Table 2 provides a layout of this section. If an SMF record provides different values for the fields than those described in the layout, the values? will be documented in the description of that SMF record.

Table 2. Common TCP/IP identification section

Offset	Name	Length	Format	Description
0(X'0')	SMF119TI_SYSName	8	EBCDIC	System name from SYSNAME in IEASYSxx

Table 2. Common TCP/IP identification section (continued)

Offset	Name	Length	Format	Description
8(X'8')	SMF119TI_SysplexName	8	EBCDIC	Sysplex name from SYSPLEX in COUPLExx
16(X'10')	SMF119TI_Stack	8	EBCDIC	TCP/IP stack name
24(X'18')	SMF119TI_ReleaseID	8	EBCDIC	z/OS Communications Server TCP/IP release identifier
32(X'20')	SMF119TI_Comp	8	EBCDIC	TCP/IP subcomponent (right padded with blanks): **CSSMTP** CSSMTP client **FTPC** FTP client **FTPD** FTP daemon **FTPS** FTP server **IDS3270** VTAM 3270 Intrusion Detection Services **IKE** IKE daemon **IP** IP layer **SMCR** Shared Memory Communications - RDMA **STACK** Entire TCP/IP stack **TCP** TCP layer **TN3270C** TN3270 client **TN3270S** TN3270 server **UDP** UDP layer
40(X'28')	SMF119TI_ASName	8	EBCDIC	Started task qualifier or address space name of address space that writes this SMF record. See specific records for deviations from this description.
48(X'30')	SMF119TI_UserID	8	EBCDIC	User ID of security context under which this SMF record is written
56(X'38')		2	EBCDIC	Reserved
58(X'3A')	SMF119TI_ASID2	2	Binary	ASID of address space that writes this SMF record (in EZASMF77 macro).
58(X'3A')	SMF119TI_ASID	2	Binary	ASID of address space that writes this SMF record (in ezasmf.h).

Table 2. Common TCP/IP identification section (continued)

Offset	Name	Length	Format	Description
60(X'3C')	SMF119TI_Reason	1	Binary	Reason for writing this SMF record: • X'C0': Interval record, more records follow • X'80': Interval record, last record in set • X'60': End-of-statistics record, more records follow • X'20': End-of-statistics record, last record in set • X'50': Shutdown starts record, more records follow • X'10': Shutdown starts record, last record in set • X'48': Event record, more records follow • X'08' : Event record, last record in set
61(X'3D')	SMF119TI_RecordID	1	Binary	Value used by the following SMF 119 records, to correlate several physical records which contain one logical set of information. The SMF 119 record descriptions will explain when the field is used. • TCP/IP profile event record (subtype 4) • TN3270E Telnet server profile event record (subtype 24) • VTAM 3270 Intrusion Detection Services event record (subtype 81)
62(X'3E')		2	EBCDIC	Reserved

VTAM 3270 Intrusion Detection Services event record (subtype 81)

The VTAM 3270 Intrusion Detection Services (IDS) function monitors 3270 data streams for primary logical units (PLUs) that are connected to the z/OS VTAM instance. Specific types of 3270 sessions can be exempted from IDS monitoring at the VTAM or application major node level if IDS monitoring is not needed for those sessions.

The 3270 IDS function monitors 3270 data streams for any attempt to write past the end of input fields or to modify protected fields. When these types of events are detected, VTAM writes a type 119 subtype 81 SMF record. This record contains information about the two end point LUs of the connection and the specific data streams that created the event.

See 3270 Intrusion Detection Services in z/OS Communications Server: SNA Network Implementation Guide for more information about the 3270 IDS function.

Assembler mappings for the structures can be found in ISTSMF77 in SYS1.MACLIB.

See Table 3 for the contents of the TCP/IP common identification section. For the 3270 IDS record, the TCP/IP common identification section indicates the following information:

SMF119TI_Stack
The name of the VTAM address space that issued this record

SMF119TI_ReleaseID
The VTAM release level found in the first 8 bytes of the ATCVT

SMF119TI_Comp
IDS3270

SMF119TI_ASName
The address space name for which this record was written

SMF119TI_UserID
User ID of security context under which this SMF record is written

SMF119TI_ASID
The address space identifier for which this record was written

SMF119TI_Reason

X'48' The event record is incomplete

X'08' The event record is complete

SMF119TI_RecordID
The last eight bits of the incident token (IST119DS_IncTk). This value might be used correlate records.

Continuing the SMF record

A set of SMF records are written for a VTAM IDS event. One SMF record is written for each saved outbound PIU. The number of saved outbound PIUs is defined by the DSCOUNT parameter. Each buffer has the SMF119TI_Reason field set to X'48' until the last or only buffer. The last buffer has the inbound PIU that caused the SMF records to be written. The SMF119TI_Reason field is set to X'08' in the last record.

Table 3 lists the contents of the 3270 IDS record self-defining section.

Table 3. 3270 IDS record self-defining section

Offset	Name	Length	Format	Description
0(X'0')	SMF119_HDR	24	EBCDIC	Standard SMF Header; subtype is 81(X'51')
Self-defining section				
24(X'18')	SMF119SD_TRN	2	Binary	Number of triplets in this record (4)
26(X'1A')		2	Binary	Reserved
28(X'1C')	SMF119IDOff	4	Binary	Offset to TCP/IP identification section
32(X'20')	SMF119IDLen	2	Binary	Length of TCP/IP identification section
34(X'22')	SMF119IDNum	2	Binary	Number of TCP/IP identification sections
36(X'24')	SMF119S1Off	4	Binary	Offset to 3270 IDS common section
40(X'28')	SMF119S1Len	2	Binary	Length of 3270 IDS common section
42(X'2A')	SMF119S1Num	2	Binary	Number of 3270 IDS common sections
44(X'2C')	SMF119S2Off	4	Binary	Offset to outbound buffer section
48(X'30')	SMF119S2Len	2	Binary	Length of outbound buffer section

Table 3. 3270 IDS record self-defining section (continued)

Offset	Name	Length	Format	Description
50(X'32')	SMF119S2Num	2	Binary	Number of outbound buffer sections
52(X'34')	SMF119S3Off	4	Binary	Offset to inbound buffer section
56(X'38')	SMF119S3Len	2	Binary	Length of inbound buffer section
58(X'3A')	SMF119S3Num	2	Binary	Number of inbound buffer sections

Table 4 lists the contents of the IDS 3270 common section.

Table 4. IDS 3270 common section

Offset	Name	Length	Format	Description
0(X'0')	IST119DS_Time	8	Binary	STCK time of the incident (UTC)
8(X'8')	IST119DS_PLUName	17	EBCDIC	PLU NetId.name
25(X'19')	IST119DS_SLUName	17	EBCIDC	SLU NetId.name
42(X'2A')		10		Reserved
52(X'34')	IST119DS_SID	8	Binary	Session Id
60(X'3C')	IST119DS_IncTk	4	Binary	Event token
64(X'40')	IST119DS_ECode	1	EBCDIC	Event error code
65(X'41')	IST119DS_DSCOUNT	1	Binary	DSCOUNT parameter
66(X'42')	IST119DS_ACTION	1	Binary	DSACTION parameter
			1111	Reserved
	IST119DS_DSACT_Rpt		.... 11..	DSACTION Report Level
	IST119DS_DSACT_SYS		.... 10..	Syslog
	IST119DS_DSACT_CON		.... 11..	Console
	IST119DS_DSACT_Int		11	DSACTION Intervention
	IST119DS_DSACT_None		01	None
	IST119DS_DSACT_Sense		10	Sense
	IST119DS_DSACT_Term		11	Term
67(X'43')		1		Reserved
68(X'44')	IST119DS_RIPV6	16	Binary	Remote IP address (TN3270 sessions only)
84(X'54')	IST119DS_RPort	2	Binary	Remote port number (TN3270 sessions only)
86(X'56')	IST119DS_Row	1	Binary	3270 display row
87(X'57')	IST119DS_Column	1	Binary	3270 display column
88(X'58')	IST119DS_Offset	2	Binary	Offset into 3270 Buffer
90(X'5A')	IST119DS_OBufO	2	Binary	Outbound buffer offset
92(X'5C')	IST119DS_IBufO	2	Binary	Inbound buffer offset

Table 4. IDS 3270 common section (continued)

Offset	Name	Length	Format	Description
94(X'5E')	IST119DS_OBufL	2	Binary	Outbound buffer length
96(X'60')	IST119DS_IBufL	2	Binary	Inbound buffer length
98(X'62')	IST119DS_OSEQ	2	Binary	Outbound PIU sequence number
100(X'64')	IST119DS_ISEQ	2	Binary	Inbound PIU sequence number
102(X'66')	IST119DS_OFLD	32	Binary	32 bytes of outbound 3270 data stream
134(X'86')	IST119DS_IFLD	32	Binary	32 bytes of inbound PIU field 3270 data stream

Table 5 lists the contents of the IDS 3270 outbound buffer section.

Table 5. IDS 3270 outbound buffer section

Offset	Name	Length	Format	Description
0(X'00')	IST119DS_DOTime	8	Binary	STCK time of the buffer (UTC)
8(X'08')	IST119DS_DOFSNF	2	Binary	First sequence number
10(X'0A')	IST119DS_DOLSNF	2	Binary	Last sequence number
12(X'0C')	IST119DS_DOOFF	2	Binary	Offset of data in DS_DORU
14(X'0E')	IST119DS_DOLen	2	Binary	Length of data in DS_DORU
16(X'10')	IST119DS_DODSBn	1	Binary	DSCOUNT buffer number
17(X'11')	IST119DS_DOFlags	2	Binary	Flags
	IST119DS_DOCData		1...	Confidential data
18(X'13')	IST119DS_DOTH	26	Binary	SNA Transmission header
45(X'2D')	IST119DS_DORH	3	Binary	SNA Request header
48(x'30')	IST119DS_DORU	4096	Binary	Outbound RU data

Note: There is one record for each outbound buffer.

Table 6 lists the contents of the IDS 3270 inbound buffer section.

Table 6. IDS 3270 inbound buffer section

Offset	Name	Length	Format	Description
0(X'00')	IST119DS_DITime	8	Binary	STCK time of the buffer (UTC)
8(X'08')	IST119DS_DIFSNF	2	Binary	First sequence number
10(X'0A')	IST119DS_DILSNF	2	Binary	Last sequence number
12(X'0C')	IST119DS_DIOFF	2	Binary	Offset of data in DS_DIRU

Table 6. IDS 3270 inbound buffer section (continued)

Offset	Name	Length	Format	Description
14(X'0E')	IST119DS_DILen	2	Binary	Length of data in DS_DIRU
16(X'10')		1	Binary	Reserved
17(X'11')	IST119DS_DIFlag	2	Binary	Flags
	IST119DS_DICData		1...	Confidential data
18(X'13')	IST119DS_DITH	26	Binary	SNA Transmission header
45(X'2D')	IST119DS_DIRH	3	Binary	SNA Request header
48(x'30')	IST119DS_DIRU	4096	Binary	Inbound RU data

Note: The inbound record is recorded in the last (or only) record.

Chapter 2. IP and SNA Codes

Session status modifiers (positions 6–8)

The following session status modifiers can appear in positions 6–8 of the session state. These can occur in any order.

Status Modifier	Meaning
/B	A session establishment request is pending.
/C	One of the session partners is a controlling LU. Modifier /C is displayed only by the SLU (that is, the host which entered the VARY LOGON).
/D	Session performing DES encryption.
/E	The 3270 Intrusion Detection Services (IDS) has found a problem with this session.
/I	Persistent session recovery is in progress.
/M	The session is capable of being recovered through multinode persistent session support.
/P	The session is a primary XRF session.
/R	Persistent session recovery is pending.
/T	Session performing Triple-DES encryption.
/U	A session termination request is pending.
/X	The session is a backup XRF session.
/CI	One of the session partners is a controlling LU and persistent session recovery is in progress. Modifier /CI is displayed only by the SLU (the host that issued the VARY LOGON).
/CP	The session is a CP-CP session.
/CR	One of the session partners is a controlling LU and persistent session recovery is pending. Modifier /CR is displayed only by the SLU (the host that issued the VARY LOGON).
/DI	Persistent session recovery is in progress, and the session uses DES encryption.
/DL	The session is a CP-SVR session.
/DR	Persistent session recovery is pending, and the session uses DES encryption.
/MD	Multinode persistent session uses DES encryption.
/MI	Multinode persistent session recovery is in progress.
/MR	Multinode persistent session recovery is pending.
/MT	Multinode persistent session uses Triple-DES encryption.
/PB	The session is a primary XRF session, and a session establishment request is pending.

/PC The session is primary XRF session, and one of the session partners is a controlling LU.

/PD Primary XRF session using DES encryption.

/PI The session is a primary XRF session, and persistent session recovery is in progress.

/PR The session is a primary XRF session, and persistent session recovery is pending.

/PT Primary XRF session using Triple-DES encryption.

/PU The session is a primary XRF session, and a session termination request is pending.

/SV The session is a SNA Service Manager session.

/TI Persistent session recovery is in progress, and the session uses Triple-DES encryption.

/TR Persistent session recovery is pending, and the session uses Triple-DES encryption.

/XB The session is a backup XRF session, and a session establishment request is pending.

/XC The session is a backup XRF session, and one of the session partners is a controlling LU.

/XD Backup XRF session using DES encryption.

/XI The session is a backup XRF session, and persistent session recovery is in progress.

/XR The session is a backup XRF session, and persistent session recovery is pending.

/XT Backup XRF session using Triple-DES encryption.

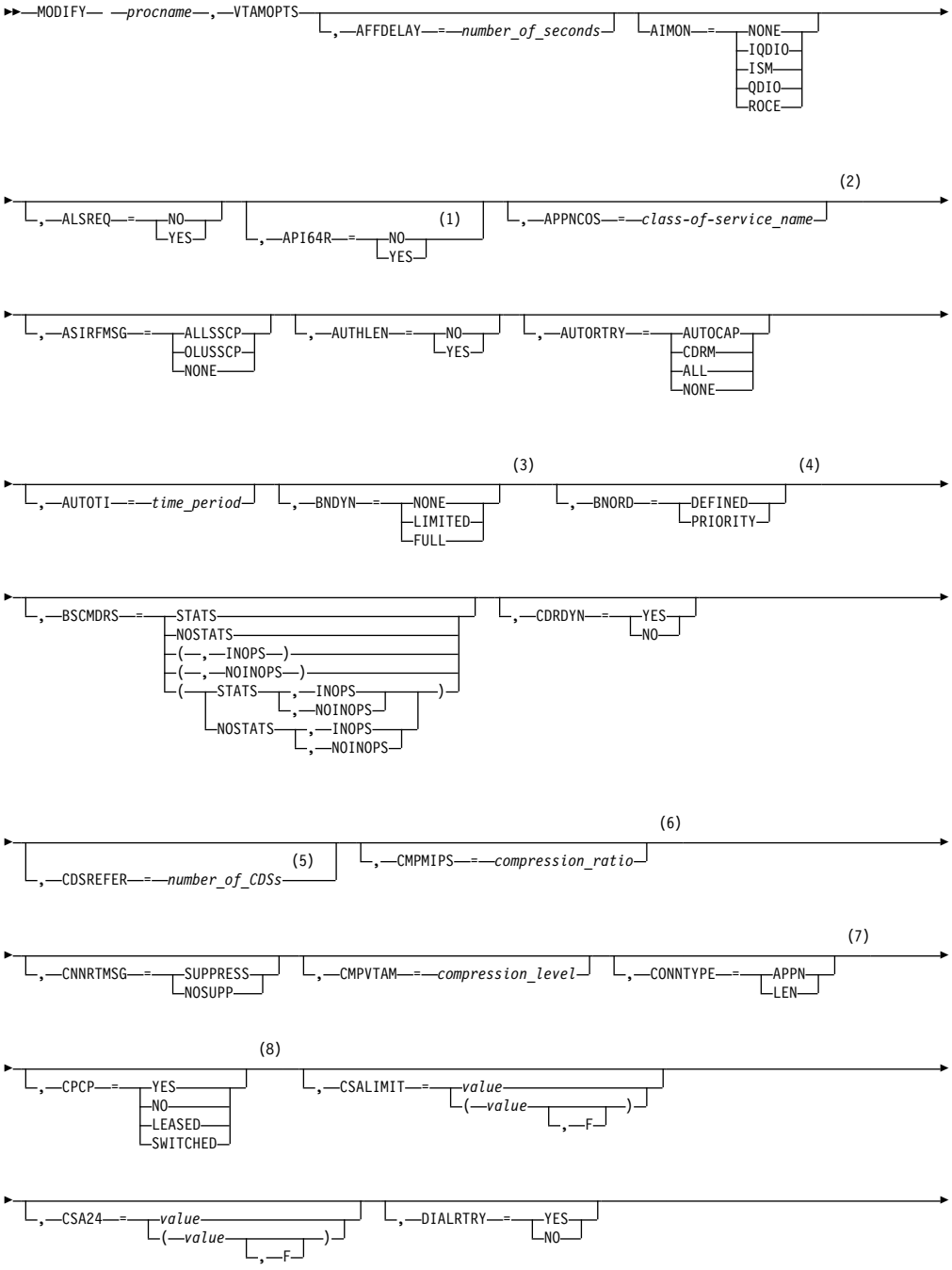
/XU The session is a backup XRF session, and a session termination request is pending.

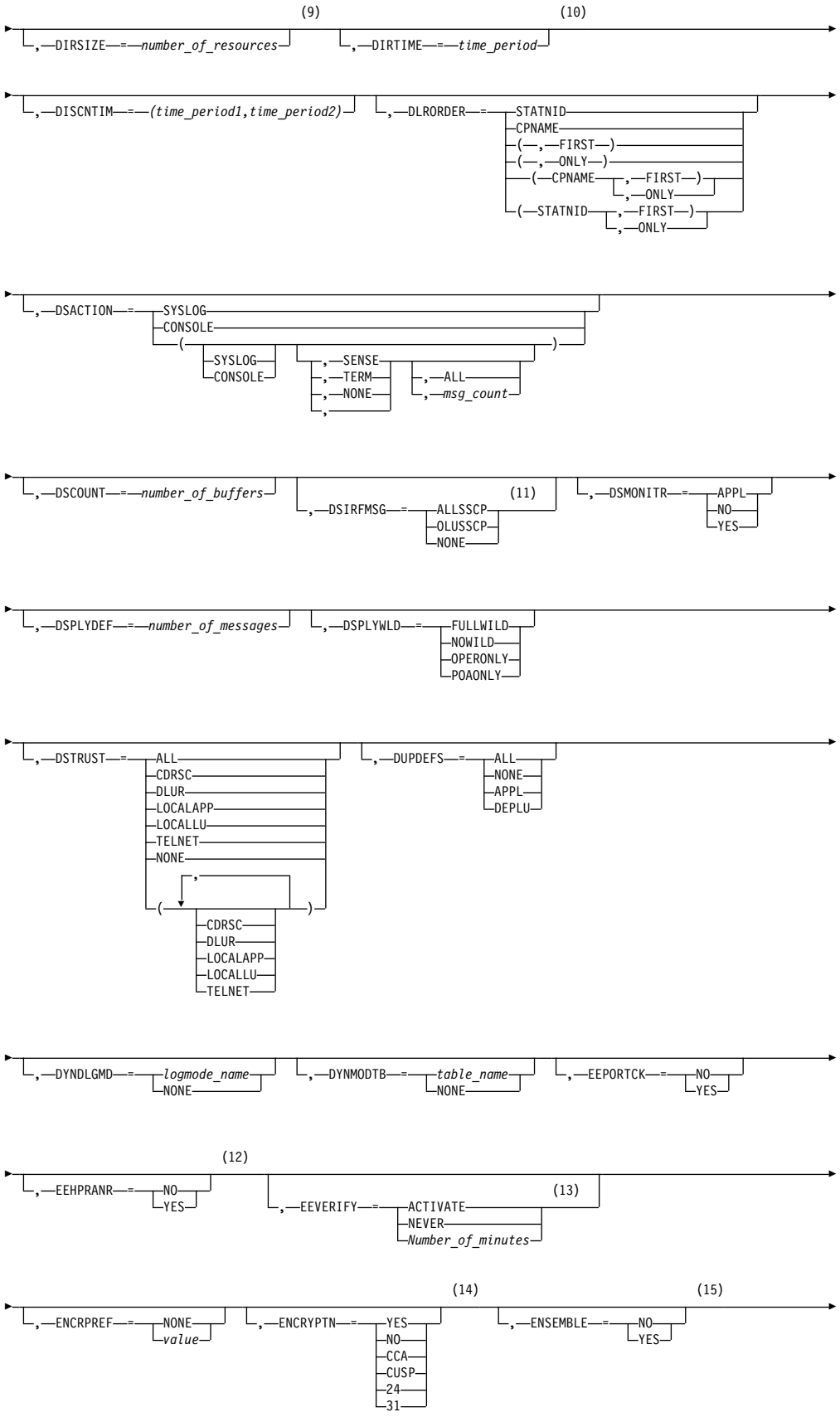
/3 The session is monitored by the 3270 IDS.

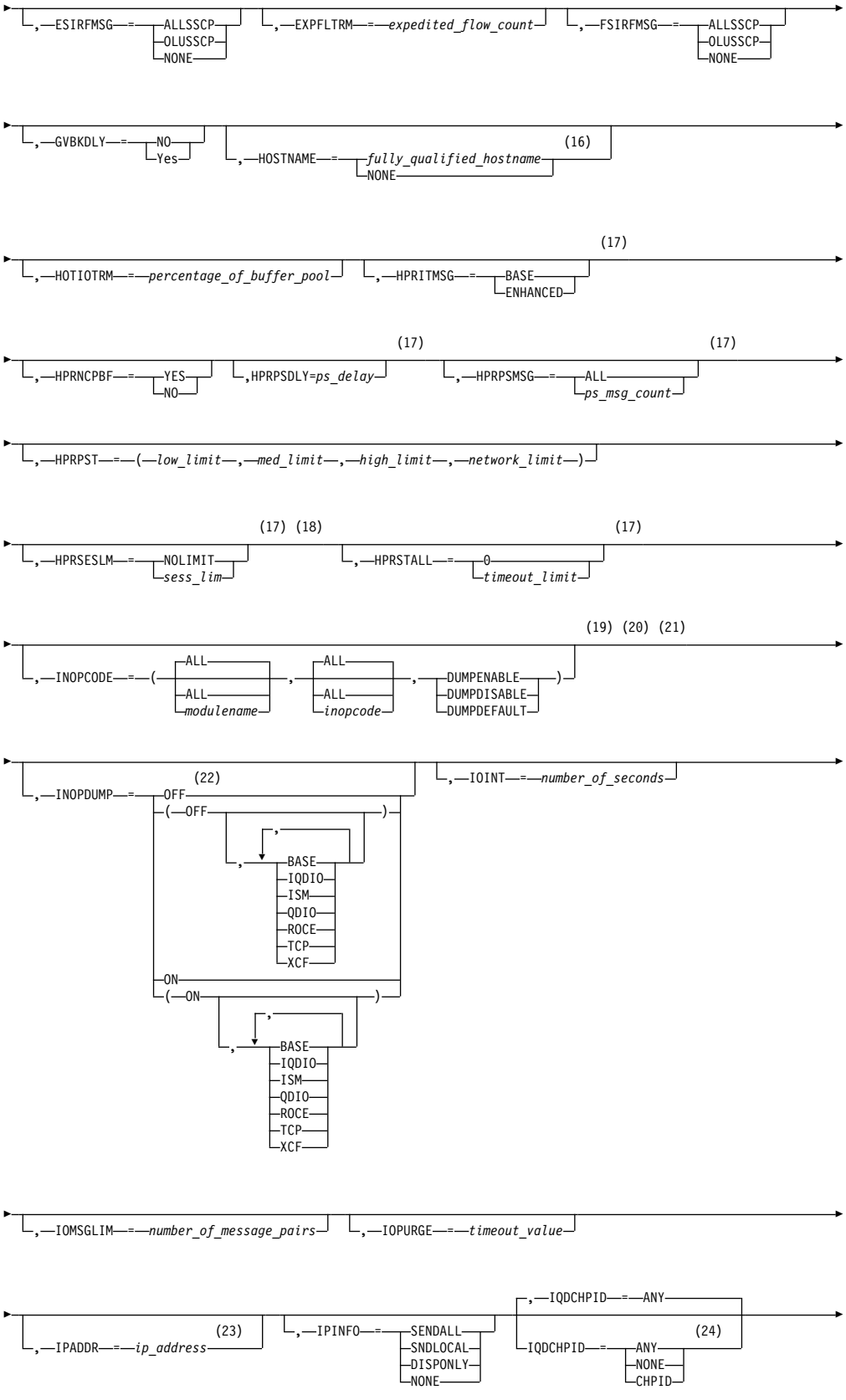
Chapter 3. Quick Reference

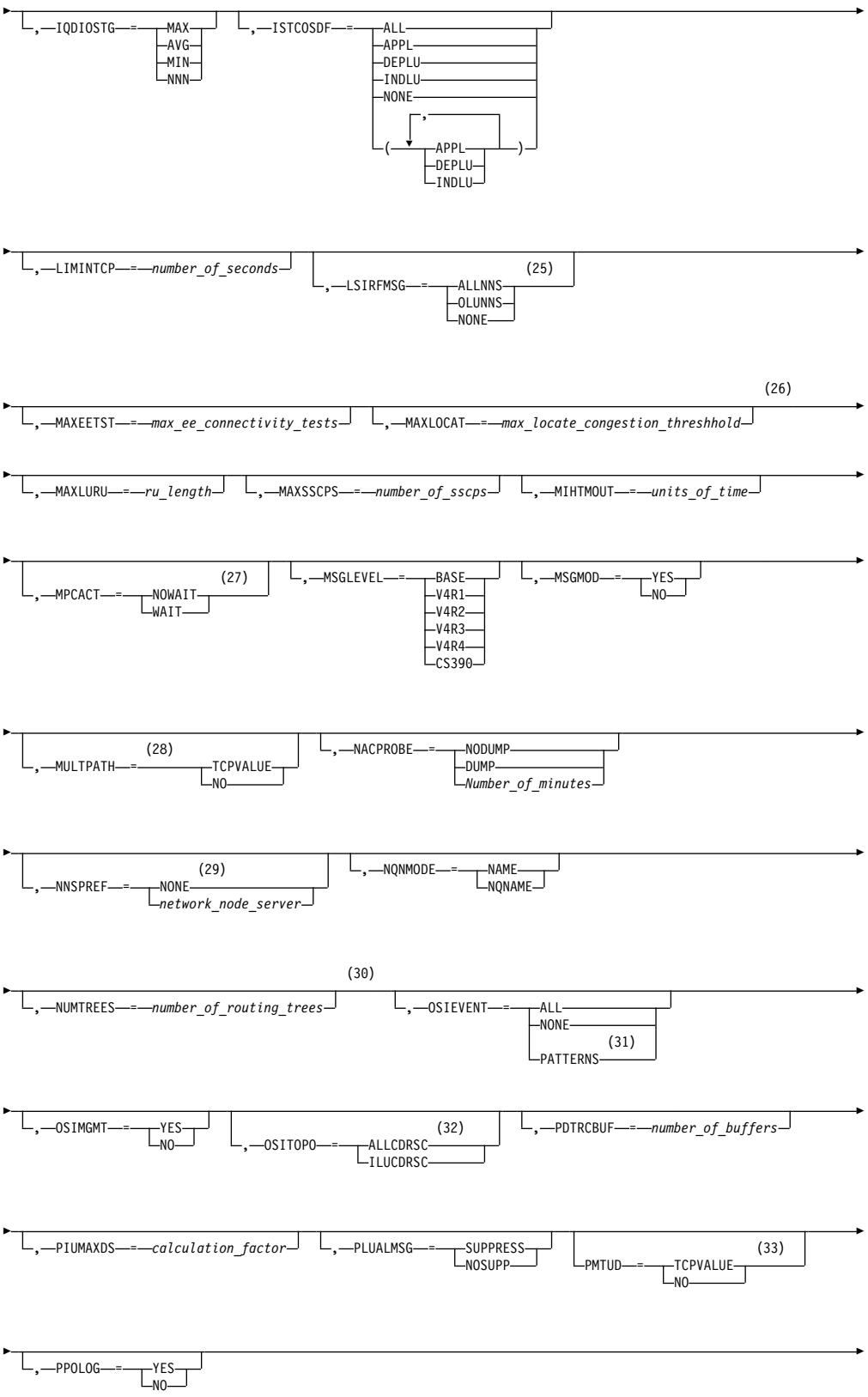
F VTAMOPTS command

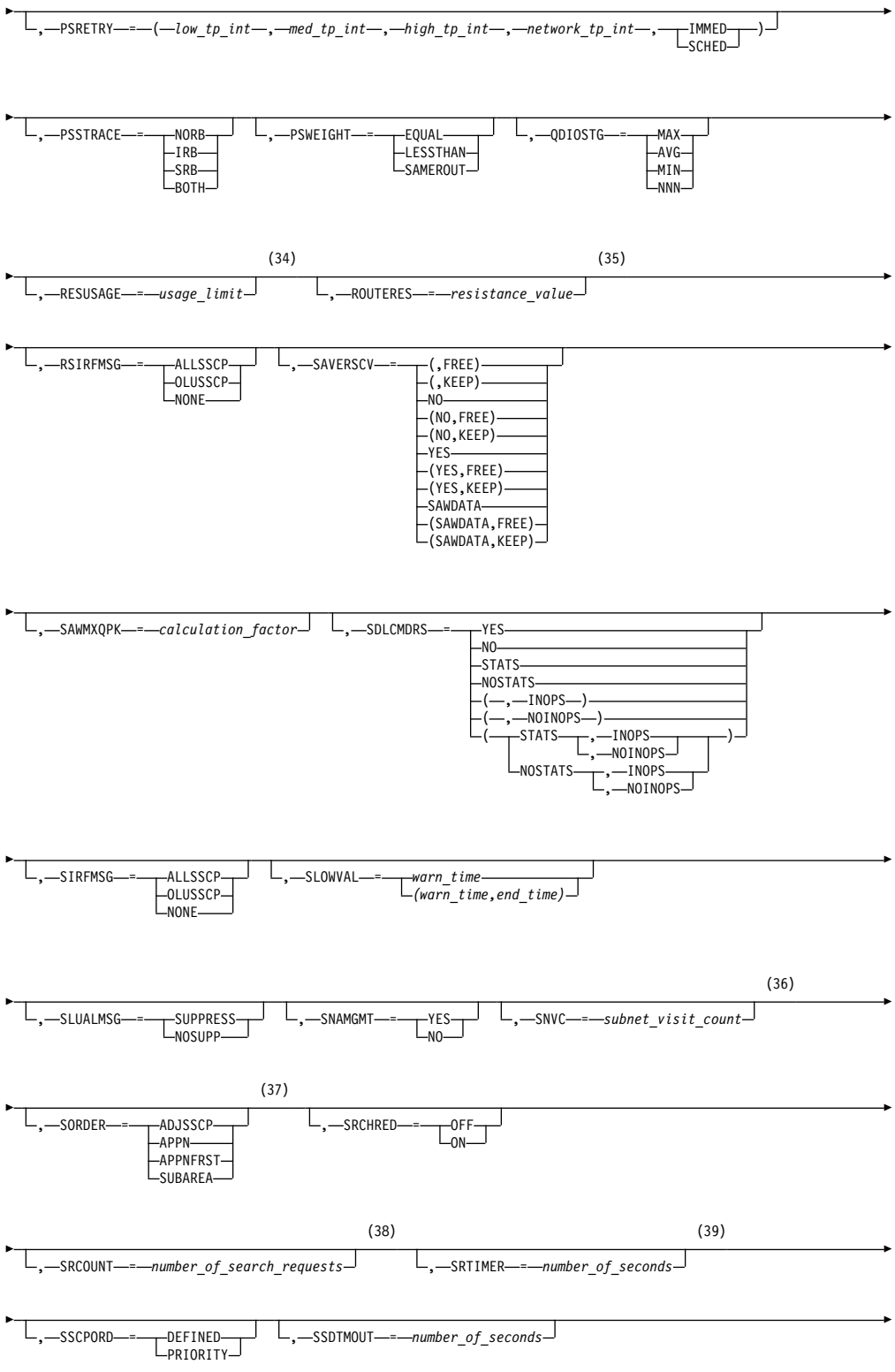
Change certain values that might have been specified on VTAM® start options:

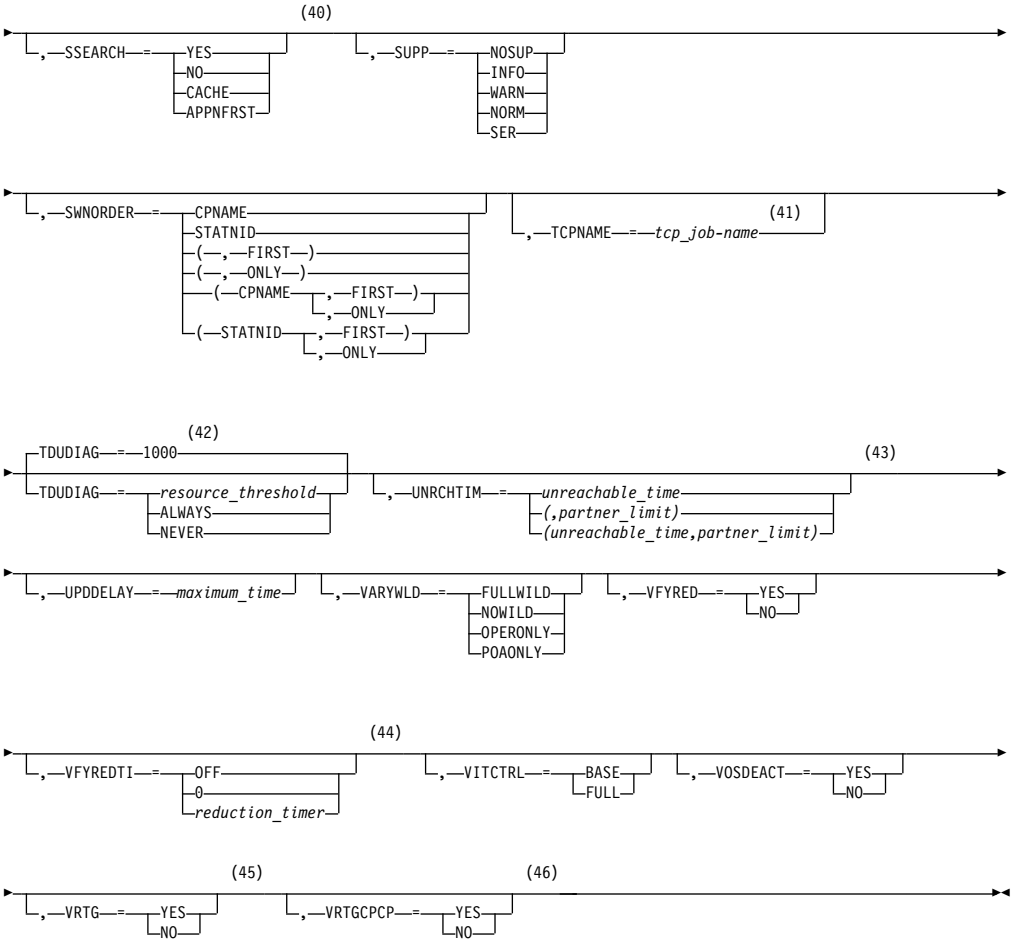



(9)
(10)
,—DIRSIZE—=—number_of_resources
,—DIRTIME—=—time_period
,—DISCNTIM—=—(time_period1,time_period2)
,—DLRORDER—=—STATNID
CPNAME
(—,—FIRST—)
(—,—ONLY—)
(—CPNAME—,—FIRST—)
,—ONLY
(—STATNID—,—FIRST—)
,—ONLY
,—DSACTION—=—SYSLOG
CONSOLE
(—SYSLOG
CONSOLE
,—SENSE
,—TERM
,—NONE
,—ALL
,—msg_count
,—DSCOUNT—=—number_of_buffers
(11)
,—DSIRFMSG—=—ALLSSCP
OLUSSCP
NONE
,—DSMONITR—=—APPL
NO
YES
,—DSPLYDEF—=—number_of_messages
,—DSPLYWLD—=—FULLWILD
NOWILD
OPERONLY
POAONLY
,—DSTRUST—=—ALL
CDRSC
DLUR
LOCALAPP
LOCALLU
TELNET
NONE
(—,—CDRSC—DLUR—LOCALAPP—LOCALLU—TELNET—)
,—DUPDEFS—=—ALL
NONE
APPL
DEPLU
,—DYNDLGMD—=—logmode_name
NONE
,—DYNMODTB—=—table_name
NONE
,—EEPORTCK—=—NO
YES
(12)
,—EEHPRANR—=—NO
YES
(13)
,—EEVERIFY—=—ACTIVATE
NEVER
Number_of_minutes
(14)
(15)
,—ENCRPREF—=—NONE
value
,—ENCRYPTN—=—YES
NO
CCA
CUSP
24
31
,—ENSEMBLE—=—NO
YES


,ESIRFMSG=ALLSSCP OLUSSCP NONE
,EXPFLTRM=expedited_flow_count
,FSIRFMSG=ALLSSCP OLUSSCP NONE
,GVBKDLY=NO Yes
,HOSTNAME=fully_qualified_hostname NONE (16)
,HOTIOTRM=percentage_of_buffer_pool
,HPRITMSG=BASE ENHANCED (17)
,HPRNCPBF=YES NO
,HPRPSDLY=ps_delay (17)
,HPRPSMSG=ALL ps_msg_count (17)
,HPRPST=(low_limit,med_limit,high_limit,network_limit)
,HPRSESLM=NOLIMIT sess_lim (17) (18)
,HPRSTALL=0 timeout_limit (17)
,INOPCODE=(ALL ALL modulename , ALL ALL inopcode , DUMPENABLE DUMPDISABLE DUMPDEFAULT) (19) (20) (21)
,INOPDUMP=OFF (OFF BASE IQDIO ISM QDIO ROCE TCP XCF) ON (ON BASE IQDIO ISM QDIO ROCE TCP XCF) (22)
,IOINT=number_of_seconds
,IOMSGLIM=number_of_message_pairs
,IOPURGE=timeout_value
,IPADDR=ip_address (23)
,IPINFO=SENDALL SNDLOCAL DISPONLY NONE
,IQDCHPID=ANY
IQDCHPID=ANY NONE CHPID (24)


,—IQDIOSTG—=—MAX
AVG
MIN
NNN
,—ISTCOSDF—=—ALL
APPL
DEPLU
INDLU
NONE
,
(—APPL—)
DEPLU
INDLU
,—LIMINTCP—=—number_of_seconds
(25)
,—LSIRFMSG—=—ALLNNS
OLUNNS
NONE
(26)
,—MAXEETST—=—max_ee_connectivity_tests
,—MAXLOCAT—=—max_locate_congestion_threshhold
,—MAXLURU—=—ru_length
,—MAXSSCPS—=—number_of_sscps
,—MIHTMOUT—=—units_of_time
(27)
,—MPCACT—=—NOWAIT
WAIT
,—MSGLEVEL—=—BASE
V4R1
V4R2
V4R3
V4R4
CS390
,—MSGMOD—=—YES
NO
(28)
,—MULTPATH—=—TCPVALUE
NO
,—NACPROBE—=—NODUMP
DUMP
Number_of_minutes
(29)
,—NNSPREF—=—NONE
network_node_server
,—NQNMODE—=—NAME
NQNAME
(30)
,—NUMTREES—=—number_of_routing_trees
,—OSIEVENT—=—ALL
NONE
(31)
PATTERNS
,—OSIMGMT—=—YES
NO
(32)
,—OSITOPO—=—ALLCDRSC
ILUCDRSC
,—PDTRCBUF—=—number_of_buffers
,—PIUMAXDS—=—calculation_factor
,—PLUALMSG—=—SUPPRESS
NOSUPP
(33)
PMTUD—=—TCPVALUE
NO
,—PPOLOG—=—YES
NO


,—PSRETRY—=—(—low_tp_int—,—med_tp_int—,—high_tp_int—,—network_tp_int—,—IMMED—)—
SCHED
,—PSSTRACE—=—NORB—
IRB—
SRB—
BOTH—
,—PSWEIGHT—=—EQUAL—
LESSTHAN—
SAMEROUT—
,—QDIOSTG—=—MAX—
AVG—
MIN—
NNN—
(34)
,—RESUSAGE—=—usage_limit—
(35)
,—ROUTERES—=—resistance_value—
,—RSIRFMSG—=—ALLSSCP—
OLUSSCP—
NONE—
,—SAVERSCV—=—(,FREE)—
(,KEEP)—
NO—
(NO,FREE)—
(NO,KEEP)—
YES—
(YES,FREE)—
(YES,KEEP)—
SAWDATA—
(SAWDATA,FREE)—
(SAWDATA,KEEP)—
,—SAWMXQPK—=—calculation_factor—
,—SDLCMDRS—=—YES—
NO—
STATS—
NOSTATS—
(—,—INOPS—)—
(—,—NOINOPS—)—
(—STATS—,—INOPS—)—
,—NOINOPS—
NOSTATS—,—INOPS—
,—NOINOPS—
,—SIRFMSG—=—ALLSSCP—
OLUSSCP—
NONE—
,—SLOWVAL—=—warn_time—
(warn_time,end_time)—
(36)
,—SLUALMSG—=—SUPPRESS—
NOSUPP—
,—SNAMGMT—=—YES—
NO—
,—SNVC—=—subnet_visit_count—
(37)
,—SORDER—=—ADJSSCP—
APPN—
APPNFRST—
SUBAREA—
,—SRCHRED—=—OFF—
ON—
(38)
,—SRCOUNT—=—number_of_search_requests—
(39)
,—SRTIMER—=—number_of_seconds—
,—SSCPORD—=—DEFINED—
PRIORITY—
,—SSDTMOUT—=—number_of_seconds—



Notes:

1 API64R can be modified only when running in z/Architecture® mode.

2 APPNCOS can be modified only if NODETYPE was specified during VTAM START processing.

3 BNDYN can be modified only if BN=YES was specified during VTAM START processing.

4 BNORD can be modified only if BN=YES was specified during VTAM START processing.

5 CDSREFER can be modified only if NODETYPE=NN and CDSERVR=NO were specified during VTAM START processing.

6 CMPMIPS is meaningful only if the value for CMPVTAM is greater than 1.

7 CONNTYPE can be modified only if NODETYPE was specified during VTAM START processing.

8 CPCP can be modified only if NODETYPE was specified during VTAM START processing.

9 DIRSIZE can be modified only if NODETYPE=NN was specified during VTAM START processing.

10 DIRTIME can be modified only if NODETYPE=NN was specified during VTAM START processing.

11 Because of the volume of messages that can be generated, it is not recommended that this option be enabled during normal operation. Instead, it is recommended that this option be enabled (using the MODIFY VTAMOPTS command) on all necessary hosts only when trying to diagnose specific problems. After the problem has been diagnosed or documentation has been collected, this option should be disabled once again (using the MODIFY VTAMOPTS command).

12 EEHPRANR is meaningful only when the NODETYPE=NN start option is also used.

13 The EEVERIFY start option is meaningful only if VTAM provides RTP-level HPR support. The EEVERIFY start option can be modified only if the NODETYPE start option is specified and the RTP value is specified on the HPR start option.

14 The ENCRYPTN start option cannot be modified if ENCRYPTN=NO was specified during VTAM START processing.

15 The ENSEMBLE setting is used to either permit or deny connectivity to the intraensemble data network and the intranode management network. The ensemble setting permits or denies connectivity by either allowing or denying activation of OSX and OSM interfaces. Modifying the ENSEMBLE start option does not cause z/OS Communications Server to take action on active OSX or OSM interfaces.

16 HOSTNAME can be modified only if NODETYPE was specified during VTAM START processing. Displays of VTAM start options will show the new value immediately; however, the new value will not be used until all Enterprise Extender lines, whose GROUP definition statements do not have HOSTNAME explicitly coded, are inactive. Any subsequent line activation from the Enterprise Extender XCA major node, whose GROUP definition statements do not have HOSTNAME explicitly coded, will make use of the new HOSTNAME start option value. The IPADDR start option, if it is in effect at the time when the MODIFY VTAMOPTS,HOSTNAME=*hostname* is specified, will be reset (that is, set to a value of 0.0.0.0) as part of the MODIFY processing. The value NONE can be used to clear the setting of the HOSTNAME start option. HOSTNAME and IPADDR cannot be modified using one MODIFY VTAMOPTS command. If both start options are specified on the same MODIFY command, they will both be ignored and message IST1917I will be generated.

17 This option is meaningful only if VTAM provides RTP-level HPR support.

18 If the current value of the HPRSESLM start option is DISABLED, then the HPRSESLM value can be changed only by stopping and restarting VTAM.

19 When specifying an InOpCode for the second parameter, always specify three digits by including any leading zeros.

20 If an InOpCode is specified for the second parameter, the first parameter cannot be ALL.

21 INOPCODE has no effect unless INOPDUMP is active for the resource when an inoperative condition is detected. See the section called MODIFY INOPCODE command in z/OS Communications Server: SNA Operation for more details.

22 When altering the INOPDUMP VTAM start option, the resulting INOPDUMP status is propagated to all TRLEs in the TRL major node if the command is globally set, or it is propogated to a subset of resources that are identified by

one or more INOPDUMP control groups. The INOPDUMP setting becomes the default status for any subsequently activated TRLEs.

23 IPADDR can be modified only if NODETYPE was specified during VTAM START processing. The new value will not be used until all lines, defined with or defaulting to the old value of the IPADDR start option, in the XCA major node used for Enterprise Extender are inactive. However, displays of VTAM start options will show the new value immediately. Any subsequent line activation from the Enterprise Extender XCA major node, whose GROUP definition statement does not specify the IPADDR operand, will make use of the new IPADDR start option value. The HOSTNAME start option, if it is in effect at the time when the MODIFY VTAMOPTS,IPADDR=*ip_address* is specified, will be reset (that is, set to a value of NONE) as part of the MODIFY processing. The value of 0.0.0.0, or an IPv6 address of all zeros, usually written as ::, can be used to clear the setting of the IPADDR start option. HOSTNAME and IPADDR cannot be modified using one MODIFY VTAMOPTS command. If both start options are specified on the same MODIFY command, they will both be ignored and message IST1917I will be generated.

24 The IQDCHPID option controls which IQD CHPID (and related subchannel devices) VTAM selects to dynamically build the iQDIO (IUTIQDIO) MPC group. The IUTIQDIO MPC group is used for TCP/IP dynamic XCF communications within System z®. Although this option can be modified (and the modification will immediately be displayed) while the IUTIQDIO MPC group is currently active, any modifications have the effects shown in the section called IQD CHPID modifications in z/OS Communications Server: SNA Operation.

25 Because of the volume of messages that can be generated, it is not recommended that this option be enabled during normal operation. Instead, it is recommended that this option be enabled (using the MODIFY VTAMOPTS command) on all necessary hosts only when trying to diagnose specific problems. After the problem has been diagnosed or documentation has been collected, this option should be disabled once again (using the MODIFY VTAMOPTS command).

26 MAXLOCAT can be modified only if NODETYPE was specified during VTAM START processing.

27 The option does not take effect for MPC groups that are in the process of being activated when the command is issued until those MPC groups are deactivated and reactivated.

28 MULTPATH is meaningful only if the NODETYPE start option is also specified.

29 NNSPREF can be modified only if NODETYPE=EN was specified during VTAM START processing.

30 NUMTREES can be modified only if NODETYPE=NN was specified during VTAM START processing.

31 OSIEVENT=PATTERNS is not valid when OSIMGMT=YES.

32 OSITOPO=ALLCDRSC is not valid when OSIMGMT=YES.

33 PMTUD is meaningful only if the NODETYPE start option is also specified.

34 RESUSAGE can be modified only if NODETYPE=NN was specified during VTAM START processing.

35 ROUTERES can be modified only if NODETYPE=NN was specified during VTAM START processing.

36 SNVC can be modified only if BN=YES was specified during VTAM START processing.

37 SORDER can be modified only if VTAM has been started as an interchange node or a migration data host.

38 SRCOUNT is meaningful only when SRCHRED=ON.

39 SRTIMER is meaningful only when SRCHRED=ON.

40 SSEARCH can be modified only if NODETYPE=NN was specified during VTAM START processing.

41 TCPNAME can be modified only if NODETYPE was specified during VTAM START processing. The new value will not be used until all lines in the XCA major node used for Enterprise Extender are inactive. However, displays of VTAM start options will show the new value immediately. Any subsequent line activation from the Enterprise Extender XCA major node will make use of the new TCPNAME value.

42 TDUDIAG is meaningful only if the NODETYPE=NN start option is also available.

43 UNRCHTIM is meaningful only if the NODETYPE start option is also used.

44 VFYREDTI can be modified only if NODETYPE=NN was specified during VTAM START processing.

45 VRTG can be modified only if NODETYPE and HOSTSA are specified.

46 VRTGCPCP can be modified only if NODETYPE and HOSTSA are specified.

Chapter 4. SNA Customization

Global storage GETBLK vector (X'000100030004')

The format of global storage GETBLK vector is shown in Table 7. One global storage GETBLK vector is built for each GETBLK subpool that exists in VTAM per request for global storage usage data. A GETBLK subpool is identified by its pool ID and buffer size. A given GETBLK pool might also be made up of multiple subpools, each of which have a different buffer size.

Table 7. Global storage GETBLK vector

Byte	Type	Description
8–15	EBCDIC, left-adjusted	Pool name
16–19	binary	Subpool buffer length
20–21	binary	Number of buffers per page
22–25	binary	Page size
26–29	binary	Number of bytes in use in subpool[1]
30–33	binary resettable	Maximum number of bytes in use in subpool since last reset[1]
34–41	binary resettable	Timestamp for maximum number of bytes in use in subpool since last reset
42–45	binary	Number of bytes allocated in subpool[1]
46–49	binary resettable	Maximum number of bytes allocated in subpool since last reset[1]
50–57	binary resettable	Timestamp for maximum number of bytes allocated in subpool since last reset

Note:

1. If bit 0 is off, these fields contain a byte count. If bit 0 is on, bits 1-31 contain a megabyte count.

Chapter 5. SNA Diagnosis Volume 2: FFST Dumps and the VIT

Trace options for the VIT

You can specify the OPTION operand in the TRACE start option or in the MODIFY TRACE command. Deactivate the VIT before you attempt to change an option; otherwise, the options that are currently in effect will remain in effect. See Deactivating the VIT for more information about deactivating the VIT.

Table 8 describes the options that you can specify on the OPTION operand. Select one or more of these options to indicate the VTAM functions you want to trace.

Table 8. Trace options of the OPTION operand

Option	Description
API option (for application programming interfaces)	This option helps you determine whether an application program is causing a problem. API entries are written for RPL macros, RPL exit routines, user exit routines, and user posts.
APIOPTS option	This option is a collection of multiple VIT options that includes all the individual VIT options required to diagnose potential application program problems. Specifying the APIOPTS option is equivalent to specifying all the following VIT options: API, MSG, NRM, PIU, PSS, SMS, and SSCP.
APPC	This option helps you determine whether an LU 6.2 application is causing a problem. LU 6.2 entries are written for APPCCMD macro invocations, user posts, and exit scheduling by LU 6.2 code, calls to a security manager for security processing, and message unit transmissions between LU 6.2 components.
APPCOPTS option	This option is a collection of multiple VIT options that includes all the individual VIT options required to diagnose potential LU 6.2 application program problems. Specifying the APPCOPTS option is equivalent to specifying all the following VIT options: API, APPC, MSG, NRM, PIU, PSS, SMS, and SSCP.
CFS option (for coupling facility interfaces)	This option helps you determine problems with the VTAM interface with the MVS coupling facility. CFS entries are written when VTAM issues MVS macros to request services related to the coupling facility.
CIA option (for channel input and output auxiliary)	This option helps you isolate problems related to channel I/O CIA entries. This option presents the remaining trace records from the CIO option.
CIO option (for channel input and output)	This option helps you isolate problems related to channel I/O. CIO entries are written for attentions, error recovery, interruptions, HALT I/O SVC, and START I/O SVC.

Table 8. Trace options of the OPTION operand (continued)

Option	Description
CMIP option (for Common Management Information Protocol Services)	Setting the CMIP option enables the following traces: • Calls from CMIP application programs to the management information base (MIB) application programming interface (API) • Calls to the read-queue exit of the CMIP application program • Topology updates from VTAM resources You can use the CMIP option to help you determine whether there is a problem in VTAM or in a CMIP application program.
CPCPOPTS option	This option is a collection of multiple VIT options that includes all the individual VIT options required to diagnose potential CP-CP session problems. Specifying the CPCPOPTS option is equivalent to specifying all the following VIT options: API, APPC, MSG, NRM, PIU, PSS, SMS, and SSCP.
CSM option (for communications storage manager events)	This option traces the parameter list information that flows across the CSM interface and key internal events (such as pool expansion and contraction) for functions that manipulate buffer states. You can trace and analyze the usage history of a buffer. You can also use the CSM trace when VTAM is not operational. An external trace is generated using the VTAM GTF event ID to write trace records directly to GTF in the same format as those recorded using VIT.
CSMOPTS option	This option is a collection of multiple VIT options that includes all the individual VIT options required to diagnose potential communications storage manager (CSM) problems. Specifying the CSMOPTS option is equivalent to specifying all the following VIT options: API, APPC, CIO, CSM, MSG, NRM, PIU, PSS, SMS, SSCP, and XBUF.
DLUROPTS option	This option is a collection of multiple VIT options that includes all the individual VIT options required to diagnose dependent LU requester (DLUR) problems. Specifying the DLUROPTS option is equivalent to specifying all the following VIT options: API, APPC, HPR, MSG, NRM, PIU, PSS, SMS, and SSCP.
EEOPTS option	This option is a collection of multiple VIT options that includes all the individual VIT options required to diagnose Enterprise Extender (EE) problems. Specifying the EEOPTS option is equivalent to specifying all the following VIT options: CIA, CIO, HPR, MSG, NRM, PIU, PSS, SMS, SSCP, and TCP.
ESC option (for execution sequence control)	This option helps you track, in detail, the flow of requests for a given process.
HPDTOPTS option	This option is a collection of multiple VIT options that includes all the individual VIT options required to diagnose high-performance data transfer (HPDT) problems. Specifying the HPDTOPTS option is equivalent to specifying all the following VIT options: CIA, CIO, HPR, MSG, PIU, PSS, SMS, and SSCP.
HPR option (for High-Performance Routing)	This option helps you isolate problems related to High-Performance Routing.

Table 8. Trace options of the OPTION operand (continued)

Option	Description
HPROPTS option	This option is a collection of multiple VIT options that includes all the individual VIT options required to diagnose High-Performance Routing (HPR) problems. Specifying the HPROPTS option is equivalent to specifying all the following VIT options: API, APPC, CIA, CIO, HPR, MSG, NRM, PIU, PSS, SMS, and SSCP.
LCS option (for local area network (LAN) channel stations)	This option helps you isolate problems that occur when an IBM® 3172 Interconnect Nways Controller is activating, deactivating, or transferring data. The LCS option enables tracing of data that VTAM receives from an IBM 3172 Interconnect Nways Controller at four levels: LCSX (channel), LCSP (port or adapter), LCSS (SAP), and LCSL (line).
LCSOPTS options	This option is a collection of multiple VIT options that includes all of the individual VIT options required to diagnose LAN channel station (LCS) problems. Specifying the LCSOPTS option is equivalent to specifying all the following VIT options: CIO, LCS, MSG, NRM, PIU, PSS, SMS, and SSCP.
LOCK option (for locking and unlocking)	This option helps you determine when VTAM modules obtain and release locks.
MSG option (for messages)	Specify this option to accomplish the following tasks: • Correlate other VIT entries with the console messages, even if you lose the console sheet. MSG entries are written for all messages to the VTAM operator. • Match the console log to a surge of activity shown in the VIT. OPER entries are written for all VTAM commands issued at an operator console.
NRM option (for network resource management)	This option helps you follow the services of the network resource management component. These services include the assignment of, references to, and the deletion of certain VTAM resources such as node names, network addresses, and control blocks. NRM entries are written for SRT macros issued by VTAM modules. CIDCTL FIND macro invocations used during the process of sending or receiving data are not traced with CDHF or CDNF trace entries unless they result in a nonzero return code.
PIU option (for path information unit flows)	This option, like the I/O and buffer contents traces, helps you isolate problems to hardware, to the NCP, or to VTAM. Unlike I/O and buffer contents traces, this option causes PIU entries to be written for all PIUs that flow internal and external to VTAM.
PSS option (for process scheduling services)	This option helps you track the flow of requests through VTAM. PSS entries are written for the VTAM macros that invoke and control PSS, scheduling, and dispatching VTAM routines.
QDIOOPTS options	This option is a collection of multiple VIT options that includes all of the individual VIT options required to diagnose queued direct I/O (QDIO) problems. Specifying the QDIOOPTS option is equivalent to specifying all the following VIT options: CIA, CIO, HPR, MSG, NRM, PIU, PSS, SMS, and SSCP.

Table 8. Trace options of the OPTION operand (continued)

Option	Description
SMS option (for storage management services)	This option helps you isolate problems caused by storage shortages. When you specify this option with the SSCP or PSS trace option, it can also help you isolate internal VTAM problems. SMS entries are written when SMS macros are used to request or free fixed-length or variable-length buffers. SMS entries are also written when VTAM expands or attempts to expand a buffer pool.
SSCP option (for system services control point request scheduling and response posting)	This option helps you isolate a VTAM problem to a specific VTAM component or module. SSCP entries are written for the request/response units (RUs) sent between VTAM components. This option also records information for the APPN CP.
STDOPTS option	This option is a collection of multiple VIT options that includes all of the individual VIT options required to diagnose problems related to high CPU, session services, Open/Close ACB, and DLCs such as multipath channel (MPC) and channel-to-channel (CTC). Specifying the STDOPTS option is equivalent to specifying all the following VIT options: API, CIO, MSG, NRM, PIU, PSS and SSCP. STDOPTS is the default trace options. When VTAM is operating in VITCTRL=FULL mode, recording for the events in the STDOPTS VIT option set is also enabled when any other group option set is enabled. Additionally during VTAM start processing with both a CSDUMP and VITCTRL=FULL start option defined, recording for the events in the STDOPTS VIT option is enabled.
TCP option (for use with Enterprise Extender)	This option is used for recording activity related to Enterprise Extender. The trace options record IP address management and timer activity.
TCPOPTS option	This option is a collection of multiple VIT options that includes all of the individual VIT options required to diagnose problems related to TCP/IP. Specifying the TCPOPTS option is equivalent to specifying all the following VIT options: CIA, CIO, MSG, NRM, PIU, PSS, SMS, SSCP, and TCP.
VCNS option (for VCNS application programming interfaces)	This option helps you determine whether a VCNS application is causing a problem. VCNS entries are written for VCNSCMD macro invocations, user posts, exit scheduling by VCNS code, and work element transmissions between VCNS components.
XBUF option (for applications that use the extended buffer list for sending and receiving data)	This option traces the contents of the extended buffer list (XBUFLST). Records are produced to trace these contents from the application-supplied extended buffer list and the internal buffer list that VTAM uses to carry the extended buffer list information. These records store relevant information contained with the extended buffer list, particularly information about CSM usage by VTAM.
XCF option (for VTAM use of the cross-system coupling facility)	Specify this option to track VTAM use of the XCF (cross-system coupling facility) MVS macro interface. Each VTAM use of an XCF macro has a VIT entry.
XCFOPTS option	This option is a collection of multiple VIT options that includes all of the individual VIT options required to diagnose cross-system coupling facility (XCF) problems. Specifying the XCFOPTS option is equivalent to specifying all the following VIT options: CIA, CIO, HPR, MSG, NRM, PIU, PSS, SMS, SSCP, and XCF.

The VIT always traces the exception conditions listed in Table 9 on page 29 and all the default VIT options listed under Activating the VIT.

Table 9. Exception conditions always traced by the VIT

Option	Exception conditions traced
APPC	• ACA and ACI entries when following commands are issued: – SEND ERROR – DEALLOC ABNDxxxx – REJECT • ACRC and ACSN entries • Other entries with nonzero return codes (except RPL6RCSC)
CFS	Entries with nonzero return codes
CIO	INOP entry
CMIP option	The following entries, when they have nonzero return codes: • MCO1 and MCO2 • MDEL • MDIS • MQRQ • MQRS • MREG • RQE
LCS	LCSL, LCSP, LCSS, and LCSX entries with nonzero reason codes
NRM	CDHF or CDNF entries with nonzero return codes
SMS	Entries with nonzero return codes and EXPN entries if a buffer pool expansion fails
SSCP	CPI, CPO, and CP2
(No option)	All SNAP entries and some exception entries[1].

Note:

1. The **** (FFST™ and PFFST), ABND, BUFF, COPY, CMER, CME2, INOP, LOST, MMG, and MM2 trace records are not activated by specific VIT options. They are activated as a result of exception conditions.

Table 10 on page 30 and Table 11 on page 31 list the VIT options and the records that they create. For more information, see the list of notes after Table 11 on page 31.

Table 10. VIT options and the records they create (API - LOCK)

VIT options	API	APPC	CFS	CIA	CIO	CMIP	CSM	ESC	HPR	LCS	LOCK
VIT records	AIx IOx RE UEx UP	ACAx ACIx ACPx ACRx ACSN ACUx MUx RACR REML REMQ USx UVx	CFAx CFCx CFDx CFEx CFFC CFLx CFNF CFPx CFRB CFTx CFUS CFVC MNPS	CCR CDSQ C64Q DEVx DRBx ENFx GCEL GCEx HCRx ICRx IDx IOSx IPLx ISPx IUTx LNKx LSNx MPDx ODPx ODTx PCIx PKx PLOQ P64Q QAPL QDIP QSRx RCPI RCPO RPLx RPST RSLK SBAx SIGA SLSx TOKx VHCR XIDx	ADE ATT ERPx HIOx INTx PCIT PCIX RDVX RIOx SIOx	MCO1 MCO2 MDEL MDIS MQRQ MQRS MREG MRGx RQE	ASNx CHGx CNTP CPYx EXPP FIXx FRBx GTBx PAGx	ESC	ARB ARBB ARBR ARPx ARQx ARSx DAPT DRPx HCLK HPRx HPRT NLPx ONLP OOSx RCM RCV REML RSCx RTP RTPx RTSx RVM RXMT	LCSx	LKEX LKSH ULKA UNLK

Table 11. VIT options and the records they create (MSG - XCF)

VIT options	MSG	NRM	PIU	PSS	SMS	SSCP	TCP	VCNS	XBUF	XCF
VIT records	MSGx OPEx QRYL TRNx	BSPx BSSx BSXx CDHx CDNx NIPx PROx RCEx SRTx	DCOx DSCx NRSx PIUx RDSx TSNS 3270 3271	ATSK BTSK DSP DTSK ETSK EXIT IRBx POST QUEx RESM SCHD SRBx VPST VRSM VWAI WAIT XPST	AREL CONT EXPN FBLx FB64 FRES FR64 GBLx GB64 GETS GT64 ORMG POOF QREx RAPx RELS REQx VTAL VTFR	AFSM ALSx AP A2 CCx CIx COx CPI CPO CP2 CPPx CPRx CPWx CRx CSx DBx DLTx ENR GNAx HLSx LDLx MT SPTx TGMx TGVx TOPx TPN2 TPTx TREx TRMx TRRx	IPAD IPGN IPG2 IPG3 IPOG IPO2 IPTC IPTM	CNA CNPx CNRx NSD VCCx VCDQ	XBAx XBIx XB6x	XCC2 XCFC XCFJ XCFL XCFM XCFR XCFS XCFX XCJ2 XCL2 XCM2 XCR2 XCS2

Note:

1. The **** (FFST and PFFST), ABND, BUFF, COPY, CMER, CME2, INOP, LOST, MMG, and MM2 trace records are not activated by specific VIT options. They are activated as a result of exception conditions.
2.
   - For CIO record types ATT, ERP, HIO, INT, SIO, with suffix I, X, or T, and INOP, the events are also captured in the NCB (pointed to by NCBCIOMV). The NCB trace table is mapped by NCBCIOAR.
   - For CIA record types INOP, RCPx, RPLx and RPST, the events are also captured in the RUNCB (pointed to by NCBCIOMV).
   - For CIA record type PCIR, the events are also captured in the SRNCB (pointed to by NCBCIOMV).
3. OON and OOX can be generated when the module trace is running.
4. For the IRBx and the SRBx records to be recorded, both the PSS trace option and the PSSTRACE start options must be specified.
5. For APPC record types REMQ and ACSN, the events are also captured in the ISTRAB.
6. Some trace records are generated only when a subtrace is active. These trace records are the HPR option record types ARBB, ARBR, the CIA option record types QAPL, QDIP, QSRx, RSLK, and the SSCP option record types HLSx,

TGVx, TRMx, and TRRx. For more information about subtraces, see z/OS Communications Server: SNA Operation.

Table 12 lists the VIT group options and the individual VIT options that are equivalent for each group option.

Table 12. VIT group options

VIT group option	Equivalent to this set of individual VIT options
APIOPTS	API, MSG, NRM, PIU, PSS, SMS, SSCP
APPCOPTS	API, APPC, MSG, NRM, PIU, PSS, SMS, SSCP
CPCPOPTS	API, APPC, MSG, NRM, PIU, PSS, SMS, SSCP
CSMOPTS	API, APPC, CIO, CSM, MSG, NRM, PIU, PSS, SMS, SSCP, XBUF
DLUROPTS	API, APPC, HPR, MSG, NRM, PIU, PSS, SMS, SSCP
EEOPTS	CIA, CIO, HPR, MSG, NRM, PIU, PSS, SMS, SSCP, TCP
HPDTOPTS	CIA, CIO, HPR, MSG, PIU, PSS, SMS, SSCP
HPROPTS	API, APPC, CIA, CIO, HPR, MSG, NRM, PIU, PSS, SMS, SSCP
LCSOPTS	CIO, LCS, MSG, NRM, PIU, PSS, SMS, SSCP
QDIOOPTS	CIA, CIO, HPR, MSG, NRM, PIU, PSS, SMS, SSCP
STDOPTS	API, CIO, MSG, NRM, PIU, PSS, SSCP
TCPOPTS	CIA, CIO, MSG, NRM, PIU, PSS, SMS, SSCP, TCP
XCFOPTS	CIA, CIO, HPR, MSG, NRM, PIU, PSS, SMS, SSCP, XCF

VTAM internal trace (VIT) record descriptions

FB64 entry for FREEB64 macro

Entry: FB64

VIT option:
SMS

Event: FreeB64 macro

VIT processing module:
ISTRACOT

Control is returned to:
ISTO64FB

This trace record shows the status of each FreeB64 request that VTAM components issue. The FreeB64 macro is the complement of the GetB64 macro. FreeB64 releases the storage that GetB64 obtains. Each GB64 entry should eventually have a corresponding FB64 entry. If the return code is not zero, this entry is generated whether the SMS option is in effect or not. This event is treated as an exception condition and, therefore, is traced whenever the VIT is active.

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
F B 6 4				ID		RTNCD	POOL	STORAGE ADDRESS								RETURN ADDRESS				FLAGS	LENGTH			SPTAE ADDRESS				RPH ADDRESS			

Byte (hex)
Contents

00-03 Record ID: C'FB64'

04-05 ID is the primary address space ID (ASID).

06 Return code

07 Possible storage pool types in hexadecimal format. For example, `86 SM3270`. For more information about storage pools, see z/OS Communications Server: SNA Network Implementation Guide.

08-0F Address of block that is freed, or 0 if FreeB64 failed.

10-13 Address of the issuer of the FreeB64 macro.

14 FBFlags

15-17 Length of storage that is freed.

18-1B Address of storage pool anchor block (SPTAE).

1C-1F Request parameter header (RPH) address.

GB64 entry for GETB64 macro

Entry: GB64

VIT option:
SMS

Event: GetB64 macro

VIT processing module:
ISTRACOT

Control is returned to:
ISTO64GB

This trace record shows the status of each GetB64 request that VTAM components issue. The FreeB64 macro is the complement of the GetB64 macro. FreeB64 releases the storage that GetB64 obtains. Each GB64 entry should eventually have a corresponding FB64 entry. If the return code is not zero, this entry is generated whether the SMS option is in effect or not. This event is treated as an exception condition and, therefore, is traced whenever the VIT is active.

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
GB64				ID		RTNCD	POOL	STORAGE ADDRESS								RETURN ADDRESS				FLAGS	LENGTH			SPTAE ADDRESS				RPH ADDRESS			

Byte (hex)
Contents

00-03 Record ID: C'GB64'

04-05 ID is the primary address space ID (ASID).

06 Return code

07 Possible storage pool types in hexadecimal format. For example, `86 SM3270`. For more information about storage pools, see z/OS Communications Server: SNA Network Implementation Guide.

08-0F Address of storage that is allocated, or 0 if GetB64 failed.

10-13 Address of the issuer of the GetB64 macro.

14 GBFlags

15-17 Length of storage that is requested, which has been rounded up to a doubleword boundary.

18-1B Address of storage pool anchor block (SPTAE).

1C-1F Request parameter header (RPH) address.

3270 entry for 3270 Intrusion Detection Services

Entry: 3270

VIT option:
PIU

Event: Internal processing during the analysis of a 3270 data stream buffer

VIT processing module:
ISTITC32

This record and the 3271 record are written during the analysis of the 3270 data steam buffer.

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
3270				ID	0	ERC	0	64-BIT ISTS3270								64-BIT ISTB3270								INC ID		SEQ NUM		RPH ADDRESS			

Byte (hex)
Contents

00–03 Record ID: C'3270'

04 ID is the primary address space ID (ASID). This field is 0 if the ASID is greater than X'FF'.

05 0

06 ERC is an error code.

07 0

08–0F 64-bit address of the session control block (ISTS3270)

10–17 64-bit address of a PIU buffer (ISTB3270)

18–19 Incident identifier

1A–1B RU sequence number field

1C–1F Request parameter header (RPH) address

3271 entry for 3270 Intrusion Detection Services

Entry: 3271

VIT option:
PIU

Event: Records when the 3270 entry is written

VIT processing module:
ISTITC32

This trace record is a continuation of the 3270 trace record. It contains the in-flight recording of events.

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
3271				INX	STCK TIME STAMP			CODE	DATA	CODE	DATA	CODE	DATA	CODE	DATA	CODE	DATA	CODE	DATA	CODE	DATA	CODE	DATA	CODE	DATA	CODE	DATA	CODE	DATA	CODE	DATA

Byte (hex)
Contents

00–03 Record ID: C'3271'

04 The index into the in-flight recording area

05–07 Bits 28 to 39 of the STCK time stamp when this record was created

08–09 A code-data pair that identifies an in-flight trace event for the session

0A–1F Additional code-data pairs

Chapter 6. SNA Messages

IST879I **{PLU{***lutype***}|SLU{***lutype***}} REAL =** *realname* **ALIAS =** *aliasname*

Explanation: This message is the first in a group of messages that VTAM issues in response to a DISPLAY SESSIONS,SID command. A complete description of the message group follows the example.

```
|   IST350I DISPLAY TYPE = SESSIONS
|   IST879I PLU{lutype} REAL = realname ALIAS = aliasname
|   IST879I SLU{lutype} REAL = realname ALIAS = aliasname
|   IST880I SETUP STATUS = status [TAKEDOWN STATUS = takedownstatus ]
|  [IST875I {ADJSSCP|ALSNAME} TOWARDS adjacent_resource_type = resource_name [text]] ...
|  [IST876I SIGNALS NEEDED TO COMPLETE SESSION {SETUP|TAKEDOWN}]
|  [IST877I signal1 [signal2] [signal3] [signal4]]
|   IST933I LOGMODE=logmode, COS=cosentry [(FROM OLU)]
|  [IST1438I LOGMODE logmode UNKNOWN IN THIS DOMAIN, DEFAULT IS ISTCOSDF]
|  [IST875I APPNCOS TOWARDS adjacent_resource_type = resource_name [text]] ...
|  [IST1048I COMPRESSION LEVEL INPUT = input_level, OUTPUT = output_level]
|  [IST1049I PERCENT REDUCTION INPUT = input_percent, OUTPUT = output_percent]
|   IST1635I {PLU|SLU} HSCB TYPE: hscbtype LOCATED AT ADDRESS X'hscbaddr'
|  [IST1635I {PLU|SLU} HSCB TYPE: hscbtype LOCATED AT ADDRESS X'hscbaddr']
|  [IST2064I PLU TO SLU RU SIZE = plu_to_slu_rusize SLU TO PLU RU SIZE = slu_to_plu_rusize ]
|  [IST2436I DSMONITR = NO]
|  [IST2437I DSMONITR = {NO|YES}, ERRORS DETECTED = errors]
|   IST1636I PACING STAGE(S) AND VALUES:
|  [IST1637I PLU--STAGE 1--SLU]
|  [IST1644I PLU--STAGE 1-----|-----STAGE 2--SLU]
|  [IST1645I PLU--STAGE 1-----|-----STAGE 2-----|-----STAGE 3--SLU]
|   IST1638I stage: PRIMARY TO SECONDARY DIRECTION - pacingtype
|  [IST1639I PRIMARY SEND: CURRENT = pscur NEXT = psnext]
|  [IST1640I SECONDARY RECEIVE = srcvcnt]
|   IST1641I stage: SECONDARY TO PRIMARY DIRECTION - pacingtype
|  [IST1642I SECONDARY SEND: CURRENT = sscur NEXT = ssnext]
|  [IST1643I PRIMARY RECEIVE = prcvcnt] ...
|  [IST1710I RSCV FROM PLU SAVED AT SESSION ACTIVATION]
|  [IST1460I TGN CPNAME TG TYPE HPR]
|  [IST1461I tgn cpname tgtype hpr]
|  [IST1713I RTP RSCV IN THE DIRECTION OF THE session_partner]
|  [IST1460I TGN CPNAME TG TYPE HPR]
|  [IST1461I tgn cpname tgtype hpr]
|  [IST1711I RSCV FROM SLU SAVED AT SESSION ACTIVATION]
|  [IST1460I TGN CPNAME TG TYPE HPR]
|  [IST1461I tgn cpname tgtype hpr]
|  [IST1713I RTP RSCV IN THE DIRECTION OF THE session_partner]
|  [IST1460I TGN CPNAME TG TYPE HPR]
|  [IST1461I tgn cpname tgtype hpr]
|  [IST1758I RSCV TOWARDS DLUR SAVED AT SESSION ACTIVATION]
|  [IST1460I TGN CPNAME TG TYPE HPR]
|  [IST1461I tgn cpname tgtype hpr]
|  [IST1759I RTP RSCV FROM THE DIRECTION OF THE DLUR]
|  [IST1460I TGN CPNAME TG TYPE HPR]
|  [IST1461I tgn cpname tgtype hpr]
|  [IST1714I NO PATH INFORMATION EXISTS]
|   IST314I END
```

IST350I

This message identifies the type of information shown in the display. For this message group, the display type is always **SESSIONS**.

IST875I

IST879I

This message displays information about an adjacent SSCP (**ADJSSCP**), adjacent link station (**ALSNAME**), or APPN Class of Service (**APPNCOS**).

VTAM(r) might issue this message twice if the issuing SSCP is an intermediate host.

adjacent_resource_type is one of the following:

DLU
The adjacent SSCP is in the direction of the destination logical unit (DLU), and a CDINIT or DSRLST is pending for the session. **DLU** applies only to adjacent SSCPs.

PLU
The adjacent SSCP or adjacent link station is in the direction of the primary logical unit (PLU).

RTP
The ALSNAME or APPNCOS is used in the direction of other endpoint of the RTP pipe.

SLU
The adjacent SSCP or adjacent link station is in the direction of the secondary logical unit (SLU).

resource_name is one of the following:

- If **ADJSSCP** or **ALSNAME** display in this message, *resource_name* is the name of the adjacent SSCP toward the indicated *adjacent_resource_type*.
- If **APPNCOS** displays in this message, *resource_name* is the APPN class of service (CoS) name.

text is not displayed when:

- The resource described in this message is an adjacent link station.
- The SSCP is not gateway capable.
- The SSCP-SSCP session is a cross-domain session.
- An APPN Class of Service name is displayed.

Possible values are:

GWNCP NAME NOT AVAILABLE
The gateway NCP name is not known to VTAM(r).

GWNCP TOWARDS *gateway_type* **=** *gwncp*
The gateway NCP name is known to VTAM(r).

Possible values are:

DLU
The gateway NCP is toward the DLU. VTAM(r) issues **DLU** only if *adjacent_resource_type* is **DLU**.

PLU
The gateway NCP is toward the PLU.

SLU
The gateway NCP is toward the SLU.

gwncp is the gateway NCP toward the *pluname* or *sluname* in message IST874I.

IST876I

This message is a header message for IST877I.

IST877I

- *signal1–signal4* are signals. They are displayed only if the session is pending session start or session end.

  The meaning of the signals is described below:

  BFSESSST-SLU
  A BFSESSST is expected from the NCP of the SLU.

CDSESSST-PLU
A cross-domain session start request is expected from the direction of the PLU.

CDSESSST-SLU
A cross-domain session start request is expected from the direction of the SLU.

SESSST-PLU
A session start request is expected from the boundary function of the PLU.

SESSST-SLU
A session start request is expected from the boundary function of the SLU.

NTFYST-GWN-PLU
Notification of a session start is expected from the gateway node in the PLU direction.

NTFYST-GWN-SLU
Notification of a session start is expected from the gateway node in the SLU direction.

The following signals are displayed only if the session is pending session end (PSESEND):

BFSESSEND-SLU
A BFSESSEND is expected from the NCP of the SLU.

CDSESSEND-PLU
A cross-domain session end request is expected from the direction of the PLU.

CDSESSEND-SLU
A cross-domain session end request is expected from the direction of the SLU.

SESSEND-PLU
A session end request is expected from the boundary function of the PLU.

SESSEND-SLU
A session end request is expected from the boundary function of the SLU.

NTFYSE-GWN-PLU
Notification of a session end is expected from the gateway node in the PLU direction.

NTFYSE-GWN-SLU
Notification of a session end is expected from the gateway node in the SLU direction.

IST879I

- *lutype* is **OLU, DLU**, or blank.
  - **OLU** is displayed if the LU is the origin session partner.
  - **DLU** is displayed if the LU is the destination session partner.
  - A blank is displayed in this field if OLU and DLU are not known because SSCP takeover has occurred. For information on takeover of of resources, see the z/OS Communications Server: SNA Network Implementation Guide
- *realname* is the network-qualified real name of the primary or secondary session partner.
- *aliasname* is the network-qualified alias name of the primary or secondary session partner. If *aliasname* is not used to locate the primary or secondary session partner, VTAM displays ***NA***.

IST880I

status is the session status. See the z/OS Communications Server: IP and SNA Codes for a description of possible session initiation and termination statuses.

takedownstatus is the session status during session termination. If session termination is not in progress, *takedownstatus* is blank. See the z/OS Communications Server: IP and SNA Codes for a description of *takedownstatus*.

IST933I

- *logmode* is the name of the entry in the logon mode table used to set up certain session parameters. These entries are rules governing how a session is to be conducted. The name specified is that known in this domain.

LOGMODE=*NA*****
LOGMODE is unknown in this domain and cannot be determined.

LOGMODE=*logmode*
LOGMODE can be determined in this domain.

LOGMODE=*BLANK*
LOGMODE can be determined in this domain and is blank. This is a valid LOGMODE entry.

- *cosentry* is the name of an entry in the subarea Class of Service table containing a list of routes allowed for a session. The COS name can be displayed in the following formats:

  COS=*NA*****
  - The subarea COS name is unknown in this domain and cannot be determined.
  - There is no subarea COS name to display because **APPNCOS** is displayed in message IST875I. If APPN session setup is not completed, the APPN COS name might not display in message IST875I. This is a temporary situation.

  COS=*cosname*
  The subarea COS name can be determined in this domain.

  COS=*BLANK*
  The subarea COS name can be determined in this domain and is blank. This is a valid COS name entry.

  COS=*cosname* **(FROM OLU)**
  The subarea COS name can be determined but is known as in the OLU domain.

IST1048I

This message is issued only if data compression is being used for this session.

input_level is the compression level used for input session traffic.

output_level is the compression level used for output session traffic.

IST1049I

This message is issued only if data compression is being used for this session.

input_percent is the percent by which input session traffic is compressed.

output_percent is the percent by which output session traffic is compressed.

If no new data has flowed since the last time you did a display, VTAM issues ***NA*** for *input_percent* and *output_percent*.

IST1438I

- This message is issued only if *logmode* is unknown in this domain and ISTCOSDF can be used as a default. See the z/OS Communications Server: SNA Resource Definition Reference and z/OS Communications Server: SNA Network Implementation Guide for more information on ISTCOSDF.
  - *logmode* is the LOGMODE displayed in message IST933I.

IST1460I

This message is a header message for information displayed in message IST1461I.

IST1461I

- The route selection control vector (RSCV) is displayed for the route to the destination node of the partner transaction program. Multiple IST1461I messages might be needed to display the full route.
- *tgn* is the transmission group number.
- *cpname* is the destination CP name for the transmission group.

  Note: The *cpname* for a composite network node might not be correct. When an SSCP takeover occurs for an NCP in a composite network node and the *cpname* was changed, the new *cpname* is not reflected in the display of the RTP end-to-end route.
- *tgtype* is the transmission group type. The values for *tgtype* can be:

  APPN Indicates that this TG is an APPN-based TG.

INTERCHANGE
Indicates that this TG represents a TG from an interchange node to a subarea node.

VRTG Indicates that this TG is a virtual-route-based TG.

ISL Indicates that this TG is an intersubnet TG.

- *hpr* is the level of HPR support provided by this node for this TG. The value displayed here depends on the HPR start option and the HPR operand on the corresponding PU definition (which can be used to override the HPR start option). The values for *hpr* can be:
  - **RTP** indicates that this node provides RTP-level HPR support.
  - **ANR** indicates that this node provides ANR-level HPR support.
  - ***NA*** indicates that this node provides no HPR support.

IST1635I

- *hscbtype* is the half-session control block type and can be one of the following:

  FMCB Function management control block. The PLU or SLU is an application on this host.

  BSB Boundary session block. The PLU or SLU is connected through an SNA channel-attached device.

  LUST Logical unit status table. The PLU is in session with a local non-SNA device on this host.

  IST1635I might be displayed multiple times, depending on the configuration. IST1635I is not displayed if the PLU or SLU is a cross-domain resource (CDRSC).
- *hscbaddr* is the hexadecimal address of the half session control block (HSCB).

IST1636I

IST1636I is a header message for the pacing messages that follow. Messages IST1638I through IST1643I might be repeated for multiple stages.

IST1637I

This message is the header message for pacing messages between the session partners when there is only one stage.

IST1638I

- This message describes the pacing stages and types that exist when transmitting data from the PLU to the SLU. The host can display up to three pacing stages. More stages might exist if the session traverses many hosts.
- *stage* indicates the pacing stage being described. For more information on pacing stages, see the z/OS Communications Server: SNA Network Implementation Guide.
- *pacingtype* can be one of the following:

  ADAPTIVE
  Adaptive pacing allows the pacing windows to expand and contract, depending on storage availability at the pacing stage boundaries.

  FIXED Fixed pacing allows a pre-negotiated number of PIUs to flow on this pacing stage before an isolated pacing response (IPR) is required to reset the window. The fixed window does not expand or contract. This pacing always uses the fixed value.

  NO PACING
  VTAM does no pacing for this stage between the SLU and the PLU. This value is only displayed for local non-SNA devices.

IST1639I

pscur represents the current pacing window between the PLU and the SLU.

psnext represents the next pacing window VTAM will use when transmitting data between the PLU and the SLU.

IST1640I

srcvcnt represents the number of PIUs the SLU can receive from the PLU.

IST1641I

- This message describes the pacing stages and types that exist when transmitting data from the SLU to the PLU. The host can display up to three pacing stages. More stages might exist if the session traverses many hosts.
- *stage* indicates the pacing stage being described. For more information on pacing stages, see the z/OS Communications Server: SNA Network Implementation Guide.
- *pacingtype* can be one of the following:

  ADAPTIVE
  Adaptive pacing allows the pacing windows to expand and contract, depending on storage availability at the pacing stage boundaries.

  FIXED Fixed pacing allows a pre-negotiated number of PIUs to flow on this pacing stage before an isolated pacing response (IPR) is required to reset the window. The fixed window does not expand or contract. This pacing always uses the fixed value.

  NO PACING
  VTAM does no pacing for this stage between the PLU and the SLU. This value is only displayed for local non-SNA devices.

IST1642I

sscur represents the current pacing window between the SLU and the PLU.

ssnext represents the next pacing window VTAM will use when transmitting data between the SLU and the PLU.

IST1643I

prcvcnt represents the number of PIUs the PLU can receive from the SLU.

IST1644I

This message is the header message for pacing messages between the session partners when there are two stages.

IST1645I

This message is the header message for pacing messages between the session partners when there are three stages.

IST1710I

This message informs users that the messages that follow describe part or all of the session path for this session as it was calculated during session activation. The session path information describes the portion of the route originating at the CP(PLU) and extending toward this node. This message group will be displayed only if session data was saved during session activation.

IST1711I

This message informs users that the messages that follow describe part or all of the session path for this session as it was calculated during session activation. The session path information describes the portion of the route originating at this node and extending toward the CP(SLU). This message group will be displayed only if session data was saved during session activation.

IST1713I

- This message informs users that the messages that follow describe the current end-to-end path of an RTP route. The route represents the portion of the total session route that uses an RTP pipe with this node as one endpoint and extending in the direction of *session_partner*. The RTP route may be different from any session route displayed in the IST1710I or IST1711I message group if RTP pathswitching has occurred since session activation; in that case, the information in message IST1713I is the more accurate information. This message group is displayed only if the session uses an RTP pipe in the direction of *session_partner*.
- *session_partner* can be one of the following:

  PLU Displays when the RTP path extends in the direction of the primary logical unit for the session.

  SLU Displays when the RTP path extends in the direction of the secondary logical unit for the session.

IST1714I

This message informs users that no session or RTP path information is available to display for this session.

IST1758I

- This message informs users that the messages that follow describe part or all of the session path for this session as it was calculated during session activation. The session path information represents a view of the session from the dependent LU requester (DLUR) node which is acting as CP(SLU). This message group will be displayed only if the following conditions are true:
  - The session involves a DLUR-owned dependent SLU.
  - The DLUR node reports the session path information for the section.
  - Session data is being saved during session activation or dependent LU activation.

IST1759I

- This message informs users that the messages that follow describe the current end-to-end path of an RTP route. The route represents the portion of the total session route that uses an RTP pipe with the Dependent LU Requester (DLUR) serving as one endpoint and extending in the direction of the CP(PLU). The RTP route may be different from the session route displayed in the IST1758I message group if RTP pathswitching has occurred since session activation; in that case, the information in message IST1759I is the more accurate information. This message group is displayed only if the following conditions are true:
  - The session involves a DLUR-owned dependent LU.
  - The session uses an RTP pipe ending at the DLUR node.
  - The DLUR node reports RTP route information for the session.
  - RTP data is being saved during session activation or dependent LU activation.

IST2064I

This message is issued only on the application owning host. Message IST1635I will display a HSCB TYPE of FMCB for the PLU, the SLU, or both, when this display is issued at the application owning host.

plu_to_slu_rusize is the RU size being used for this session from the primary logical unit (PLU) to the secondary logical unit (SLU).

slu_to_plu_rusize is the RU size being used for this session from the secondary logical unit (SLU) to the primary logical unit (PLU).

If either RU size is defaulted to or coded as 0, this indicates that there is no limit to the RU size. For this case, the message will actually display a value of 65535 because this is the largest supported RU size.

IST2436I

This message is issued only on an application owning host. Message IST2436I indicates that the 3270 Intrusion Detection Services is not monitoring this session.

IST2437I

This message is issued only on an application owning host. Message IST2437I indicates the status of the 3270 Intrusion Detection Services for this session.

In the message text:

NO Indicates that the 3270 Intrusion Detection Services is no longer monitoring this session.

YES Indicates that the 3270 Intrusion Detection Services is currently monitoring this session.

errors The number of errors in the 3270 data stream that has been detected for this session.

System action: Processing continues.

Operator response: If message IST1438I is displayed and the default logmode is not desired, collect the system log for problem determination.

System programmer response:

If message IST1438I is not displayed, no action is necessary.

If message IST1438I is displayed, and *logmode* (instead of ISTCOSDF) should have been known in this domain, verify that *logmode* is in the LOGMODE table associated with the SLU or in the default LOGMODE table ISTINCLM.

IST1242I POOL CURRENT MAXIMUM [POOL CURRENT MAXIMUM]

Explanation: This message is the first message in a group of messages that VTAM issues in response to a DISPLAY STORUSE command.

Examples of possible message groups follow.

- DISPLAY STORUSE,POOL=*poolname*

  This message group displays information for a specific storage pool.

```
 IST350I  DISPLAY TYPE = STORAGE USAGE
 IST1242I POOL     CURRENT  MAXIMUM
 IST1243I poolname current  maximum
[IST1315I DISPLAY TRUNCATED AT keyword = number]
 IST1454I 1 POOL(S) DISPLAYED
 IST314I  END
```

- DISPLAY STORUSE,POOL=* command.

  This message group displays storage usage for all storage pools, including summary information for storage pools and modules.

```
IST350I  DISPLAY TYPE = STORAGE USAGE
 IST1242I POOL     CURRENT MAXIMUM   [POOL     CURRENT MAXIMUM]
 IST1243I poolname current  maximum   [poolname current  maximum]
[IST1315I DISPLAY TRUNCATED AT keyword = number]
 IST1454I 1 POOL(S) DISPLAYED
 IST924I -------------------------------------------------------------
 IST1244I TOTAL    storage_type   POOL STORAGE USAGE:   current maximum
 IST1244I TOTAL    storage_type   POOL STORAGE USAGE:   current maximum
 IST1244I TOTAL    storage_type   POOL STORAGE USAGE:   current maximum
 IST924I -------------------------------------------------------------
[IST981I VTAM PRIVATE: CURRENT = currentK, MAXIMUM USED = maximumK]
 IST924I -------------------------------------------------------------
 IST1565I type    MODULES = currentK
 IST1565I type    MODULES = currentK
 IST1565I type    MODULES = currentK
 IST314I  END
```

IST350I

This message identifies the type of information in the display and is always **STORAGE USAGE** for this message group.

IST981I

*current*K is the amount of VTAM private storage currently in use. This does not include the amount of private storage required to load the VTAM modules.

*maximum*K is the maximum amount of VTAM private storage ever in use since VTAM was started.

See the z/OS Communications Server: SNA Network Implementation Guide for more information about storage pools.

If this message does not appear in the display, you may need to reissue the DISPLAY STORUSE command, specifying a higher value for the MAX operand. See the z/OS Communications Server: SNA Operation for additional information.

IST1242I

This message is a header message for the information displayed in message IST1243I.

IST1243I

poolname is the name of the storage pool specified on the DISPLAY STORUSE command.

current is the total current storage usage, in kilobytes, for storage pools[1].

maximum is the total maximum storage usage, in kilobytes, for storage pools since VTAM was initialized[1].

IST1244I

storage_type is either **PRIVATE** (private storage), **COMMON** (common storage), or **HVCOMM** (High Virtual Common).

current is the total current storage usage for storage pools and is expressed in kilobytes[1].

maximum is the total maximum storage usage since VTAM was initialized, and is expressed in kilobytes[1].

IST1315I

VTAM issues this message when the number of pools to be displayed exceeds the value specified for the MAX or NUM operand.

keyword is either **MAX** or **NUM**.

number is the value specified for either the MAX or NUM operand.

IST1454I

This message shows the total number of storage pools for which storage usage information is displayed.

IST1565I

- *type* can be one of the following:

  CSA 31-bit and 24-bit addressable common storage acquired for VTAM modules

  CSA24 24-bit addressable common storage acquired for VTAM modules

  PRIVATE
  Private storage used to load VTAM modules
- *currentK* is the current VTAM CSA allocation for modules.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Routing code: 2

Descriptor code: 5

IST1244I TOTAL *storage_type* **POOL STORAGE USAGE:** *current maximum*

Explanation: This message is part of a group of messages that VTAM issues in response to a DISPLAY STORUSE,POOL=* command requesting storage usage for all private, common, and high virtual common storage pools. See IST1242I for a complete description of this message group.

storage_type is either **PRIVATE** (private storage), **COMMON** (common storage), or **HVCOMM** (High Virtual Common).

current is the total current storage usage, and is expressed in kilobytes[1].

maximum is the total maximum storage usage since VTAM was initialized, and is expressed in kilobytes[2].

System action: Processing continues.

Operator response: None.

System programmer response: None.

Routing code: 2

Descriptor code: 5

---

1. High virtual common storage *current* and *maximum* values might exceed 9999999 kilobytes (approximately 10 gigabytes). If they do, 9999999 is displayed.

2. High virtual common storage *current* and *maximum* values might exceed 9999999 kilobytes (approximately 10 gigabytes). If they do, 9999999 is displayed.

IST1345I ID VALUE DESCRIPTION

Explanation: VTAM issues this message as part of a group of messages in response to a DISPLAY STATS,TYPE=VTAM command.

Notes:

1. The information in this display may be used to calculate storage requirements for VTAM. See the z/OS Communications Server: New Function Summary for information about storage requirements for VTAM.
2. For a description of the DISPLAY STATS command, see the z/OS Communications Server: SNA Operation.

A complete description of the message group follows the example.

```
 IST350I  DISPLAY TYPE = STATS,TYPE=VTAM
 IST1349I COMPONENT ID IS dddd-ddddd-ddd
 IST1345I    ID VALUE        DESCRIPTION
 IST1227I ddddd value      = description
:
[IST1315I DISPLAY TRUNCATED AT keyword = number]
 IST1454I count STATISTICS DISPLAYED
 IST314I  END
```

IST350I

This message identifies the type of information in the display and is always **STATS,TYPE=VTAM** for this message group.

IST1227I

- *ddddd* is a storage estimates function ID number assigned by VTAM. It can be up to five digits in length and is displayed without leading zeros.
- Possible function ID numbers and their descriptions follow:

  2 *value* **= VIT TABLE SIZE**
  value represents the number of megabytes allocated for the VTAM internal trace table.

  5 *value* **= CHANNEL-ATTACHED CONTROLLERS**
  value represents the number of channel-attached communication controllers that are defined to and owned by this VTAM. *value* includes one resource internally defined by VTAM.

  6 *value* **= MAXBFRU FOR CHANNEL-ATTACHED CONTROLLERS**
  value represents the sum of the values coded for the MAXBFRU operands for all channel-attached communication controllers defined to this VTAM.

  7 *value* **= INTERCONNECT CONTROLLERS FOR** *majornode*
  value represents the number of IBM 3172 Interconnect Controllers defined in this VTAM for *majornode*.

  8 *value* **= XCA MAJOR NODES** *majornode*
  value represents the number of external communication adapters defined in this VTAM with VBUILD, TYPE=XCA definition statements.

  9 *value* **= 3172 CONNECTIONS FOR** *majornode*
  value represents the number of unique CUADDR operands specified on the PORT definition statements for external communication adapter (XCA) *majornode*.

  10 *value* **= TOTAL LINE STATEMENTS FOR XCA MAJOR NODES**
  value represents the number of LINE statements for all external communication adapter (XCA) major nodes.

  11 *value* **= CHANNEL-TO-CHANNEL ATTACHMENTS**
  value represents the number of channel-to-channel (CTC) lines that are defined to VTAM with VBUILD,TYPE=CA definition statements and GROUP definition statements that specify LNCTL=CTCA. Multipath channel attached resources are included under **ID 120**.

  12 *value* **= TOTAL MAXBFRU FOR CTC ATTACHMENTS**
  value represents the sum of the values coded for all MAXBFRU operands for channel-to-channel (CTC) attachments defined in this VTAM.

13 *value* **= CTC TOTAL MAXBFRU CROSS DOMAIN**
value represents the sum of the values coded for all MAXBFRU operands for channel-to-channel (CTC) attachments to this VTAM but defined in other VTAMs.

14 *value* **= CA CLUSTER CONTROLLER TOTAL**
value represents the number of cluster controllers that are channel attached to this VTAM.

15 *value* **= SNA PU TOTAL MAXBFRU**
value is the sum of the values coded for all MAXBFRU operands for channel attached SNA PUs activated from this VTAM.

16 *value* **= LOCAL NON-SNA TERMINALS**
value represents the number of local non-SNA terminals that are defined on LOCAL definition statements that are part of local non-SNA major nodes.

17 *value* **= NETVIEW PIU TRACE BUFFER SIZE**
value represents the size of the NetView® PIU trace buffers.

18 *value* **= NETVIEW PIU TRACE BUFFERS**
value represents the number of NetView PIU trace buffers.

19 *value* **= NETVIEW SAW BUFFER SIZE**
value represents the size of all NetView session awareness (SAW) buffers.

20 *value* **= NETVIEW SAW BUFFERS**
value represents the number of NetView session awareness (SAW) buffers.

21 *value* **= ICA DEVICES**
value represents the number of integrated communication-adapter (ICA) devices.

22 *value* **= DESTINATION SUBAREAS**
value represents the number of unique type 4 and 5 nodes with which this VTAM will communicate. *value* always includes one resource internally defined by VTAM.

45 *value* **= DEPENDENT LU TOTAL FOR** *majornode*
value represents the total number of dependent LUs defined under *majornode* with VBUILD, TYPE=LOCAL coded.

46 *value* **= INDEPENDENT LU TOTAL**
value represents the total number of independent LUs for which VTAM will provide boundary function services.

47 *value* **= MAXIMUM SUBAREA**
value represents the maximum subarea number allowed in this SSCP.

48 *value* **= DEFINED PU TOTAL**
value represents the total number of PUs that are defined in this VTAM.

49 *value* **= ACTIVE PU TOTAL**
value represents the total number of PUs that are active in VTAM.

50 *value* **= DEFINED LU TOTAL**
value represents the number of device type LUs defined in this VTAM.

51 *value* **= ACTIVE LU TOTAL**
value represents the total number of LUs that are active in VTAM.

52 *value* **= ACTIVE DEPENDENT LU TOTAL**
value represents the total number of dependent LUs that are active under a VBUILD TYPE=LOCAL major node.

53 *value* **= LOCAL LU-LU SESSIONS**
value represents the number of sessions with one or both session partners defined to this VTAM under VBUILD,TYPE=LOCAL major nodes.

54 *value* **= PERSISTENT LU-LU SESSIONS**
value represents the number of sessions that exist with persistent LU-LU session-capable applications owned by this VTAM.

55 *value* **= LU TOTAL TSO SESSIONS**
value represents the number of sessions with a time-sharing option (TSO) application program running on this VTAM. This includes local, cross-domain, and cross-network resources.

56 *value* **= TOTAL APPL SESSIONS**
value represents the number of sessions with application programs running on this VTAM. This includes local, cross-domain, and cross-network resources.

57 *value* **= LU6.2 APPLICATIONS**
value represents LU 6.2 applications that will open an application control block (ACB) in this VTAM. If the node being displayed supports APPN, *value* always includes one resource internally defined for APPN.

58 *value* **= LU6.2 SESSIONS**
value represents LU 6.2 sessions with application LUs that are owned by this VTAM.

60 *value* **= ICSF ENCRYPTION SERVICES**
value represents the total number of LU-LU sessions as well as sessions between an application and another LU that will use ICSF encryption services. The ENCR operand on the APPL definition statement must be specified as REQD, COND, SEL, or OPT. The ENCR operand on the LU definition statement must be specified as REQD or OPT for encryption to be used.

61 *value* **= SNA DATA COMPRESSION SESSIONS**
value represents the number of sessions that will use SNA data compression functions.

63 *value* **= RECOVERABLE SESSIONS**
value represents the number of sessions to be recovered during a network failure. *value* includes all SSCP-LU and LU-LU sessions.

64 *value* **= CURRENT NUMBER OF SESSION PARTNERS**
value represents the total number of LUs, applications, and cross-domain resources that are currently in session.

65 *value* **= NUMBER OF LINES DEFINED**
value represents the number of lines defined on LINE statements that are owned by this VTAM. *value* includes all NCP lines owned by this SSCP as well as all lines defined under VTAM major nodes.

66 *value* **= SWNET STATEMENTS**
value represents the number of VBUILD statements for this VTAM that have TYPE=SWNET specified. *value* always includes one statement internally defined by VTAM.

67 *value* **= PU STATEMENTS UNDER SW LINES**
value represents the number of PU statements under all group statements that have DIAL=YES specified.

68 *value* **= MAXNO OPERAND**
value represents the sum of values coded for the MAXNO operand on all VBUILD TYPE=SWNET definition statements.

69 *value* **= MXGRP OPERAND**
value represents the sum of values coded for the MXGRP operand on all VBUILD TYPE=SWNET definition statements. VTAM adds 1 to *value* for each group statement in the major node.

70 *value* **= PATH STATEMENTS**
value represents all PATH definition statements under all PUs defined for switched major nodes.

71 *value* **= LU-APPL SESSIONS**
value represents the number of LUs owned by this VTAM in session with an application program owned by this VTAM (for example, a terminal logged on to CICS®). *value* includes all dynamically defined LUs.

73 *value* **= SAME NETWORK MULTI-NODE LU SESSIONS**
value represents the number of non-LU 6.2 sessions in which one LU is owned by this VTAM and the other LU is owned by another node or VTAM in the same network.

74 *value* **= CROSS NETWORK APPL SESSIONS**
value represents the number of cross-network sessions between an application program in this VTAM and a resource owned by a VTAM in another network.

77 *value* **= SAME DOMAIN LU6.2 SESSIONS**
value represents LU 6.2 sessions in which both LUs are owned by this VTAM.

78 *value* **= SAME NETWORK MULTI-NODE LU6.2 SESSIONS**
value represents the number of LU 6.2 sessions in which one LU is owned by this VTAM and the other LU is owned by another node or VTAM in the same network.

79 *value* **= CROSS NETWORK LU6.2 SESSIONS**
value represents the number of LU 6.2 sessions in which one LU is owned by this VTAM and the other LU is owned by a VTAM in another network.

80 *value* **= NETWORK INDEPENDENT LU TOTAL**
value represents the number of independent LUs either locally, remotely or CDRSC defined. All independent LUs will be represented as CDRSCs by VTAM.

81 *value* **= DYNAMICALLY DEFINED LU TOTAL**
value represents the number of dependent LUs which will be dynamically defined to PUs which are capable of receiving PSIDs (for example, 3174) when they are powered on.

99 *value* **= VTAM CONFIGURATION .**
value represents the node type in the VTAM start parameters. If the node type has not been specified, *value* will be **SUBAREA**.

100 *value* **= DYNAMIC DIRECTORY ENTRIES**
value represents the number of different LUs and CPs this VTAM needs to locate or access for session establishment or network management. If this VTAM is a central directory server, *value* also includes all resources that have been centrally registered with this VTAM.

101 *value* **= CENTRAL DIRECTORY SERVER SUPPORT**
value represents the value specified for CDSERVR in the VTAM start parameters.

- If *value* represents **CDSERVR=YES**, this VTAM is a central directory server for the network.
- If *value* represents **CDSERVR=NO**, this VTAM is not a central directory server for the network.

102 *value* **= REGISTERED DIRECTORY ENTRIES**
value represents the number of different destination LUs and CPs of other nodes that are registered to this VTAM. If VTAM supports APPN, *value* always includes one resource internally defined for APPN.

103 *value* **= SYSTEM DEFINED DIRECTORY ENTRIES**
value represents the number of different destination LUs and CPs that are system defined in the VTAMLIST for this VTAM.

104 *value* **= ADJACENT END NODES**
value represents the number of end nodes that have established CP-CP sessions with this VTAM.

106 *value* **= CENTRAL DIRECTORY SERVER**
value represents the number of central directory servers which exist in this network.

107 *value* **= ADJACENT NETWORK NODES**
value represents the number of network nodes which have established CP-CP sessions with this VTAM.

108 *value* **= APPN CLASS OF SERVICE**
value represents the total number of APPN classes of service defined in this VTAM.

109 *value* **= NETWORK NODES IN THE NETWORK**
value represents the total number of network nodes known to this VTAM.

111 *value* **= CONNECTION NETWORKS**
value represents the total number of connection networks (virtual nodes) known to this VTAM.

112 *value* **= SAME NETWORK MULTI-NODE APPL SESSIONS**
value represents the number of non-LU 6.2 sessions between application programs in this VTAM and LUs owned by another node or VTAM in the same network (for example, CICS in session with a terminal owned by another VTAM).

113 *value* **= PARALLEL SESSION PER LU**
value represents the average number of sessions for each LU with applications owned by this VTAM.

116 *value* **= INTERMEDIATE ROUTED SESSIONS**
value represents the number of sessions that this VTAM handles or routes for which neither session partner is defined to this VTAM.

119 *value* **= CROSS NETWORK LOGICAL UNIT SESSIONS**
value represents the number of non-6.2 LUs owned by this VTAM in session with a resource owned by another node or VTAM in another network (for example, a terminal logged onto CICS in another network).

120 *value* **= MULTIPATH CHANNEL MAJOR NODES**
value represents the number of channel-attached major nodes with multipath channel (MPC) support. MPC major nodes contain VBUILD,TYPE=CA definition statements with GROUP,LNCTL=MPC in the definition statement.

121 *value* **= MPC READ SUBCHANNEL ADDRESSES**
value represents the number of subchannel addresses with READ= specified on the LINE definition statement defined for a channel-attached major node for MPC support.

122 *value* **= MPC WRITE SUBCHANNEL ADDRESSES**
value represents the number of subchannel addresses with WRITE= specified on the LINE definition statement defined for a a channel-attached major node for MPC support.

123 *value* **= MPC READ BUFFER**
value represents MAXBFRU for all READ subchannels defined in this VTAM. The same MAXBFRU value should be used for all READ subchannels that are defined in the same MPC major node. The number entered indicates the number of pages VTAM allocates to receive data on the MPC CTC connection.

124 *value* **= MPC WRITE BUFFER**
value represents the sum of MAXBFRU for all WRITE subchannels defined in the adjacent VTAMs that are channel attached to this VTAM for MPC support. WRITE subchannel buffer size is dependent on the MAXBFRU value for READ subchannel on the other side of VTAM. The same MAXBFRU value should be used for all WRITE subchannels that are defined in the same MPC major node. The number entered indicates the number of pages VTAM allocates to send data on the MPC CTC connection.

125 *value* **= APPLICATION SESSIONS**
value represents the number of sessions in which both session partners are applications defined to this VTAM.

140 *value* **= MAXIMUM DIRECTORY SIZE**
value represents the value specified or defaulted for the DIRSIZE start option.

141 *value* **= MAXIMUM TRS ROUTING TREES**
value represents the value specified or defaulted for the NUMTREES start option.

142 *value* **= END NODE TRANSMISSION GROUPS**
value represents the number of APPN transmission groups between this node and attached end nodes.

143 *value* **= NETWORK NODE TRANSMISSION GROUPS**
value represents the number of APPN transmission groups between this node and attached network nodes.

144 *value* **= VIRTUAL NODE TRANSMISSION GROUPS**
value represents the number of APPN transmission groups between this node and attached virtual nodes.

151 *value* **= DEPENDENT LU TOTAL FOR** *majornode*
value represents the total number of dependent LUs defined in a PU type 4 or 5 major node.

152 *value* **= ACTIVE DEPENDENT LU REQUESTERS**
value represents the number of dependent LU requesters currently being served by this VTAM dependent LU server.

153 *value* **= ACTIVE DLUR SERVED PU TOTAL**
value represents the total number of physical units owned by the dependent LU requesters served by this VTAM dependent LU server.

154 *value* **= ACTIVE DLUR SERVED LU TOTAL**
value represents the number of dependent logical units owned by the dependent LU requesters served by this VTAM dependent LU server.

155 *value* **= VR-BASED TRANSMISSION GROUPS**
value represents the number of virtual-route-based transmission groups between this node and other VTAM CDRMs.

156 *value* **= CONNECTION NETWORK DYNAMIC TGS**
value represents the number of dynamic transmission groups activated by this node for use with connection networks. VTAM will create these dynamic transmission groups when both of the following exist:

- A session is established between this VTAM and another node connected via the same virtual node.
- There is no existing predefined line to the other node.

157 *value* **= TRANSPORT RESOURCE LIST ENTRIES**
value represents the number of transport resource list entries (TRLEs) active in this VTAM.

159 *value* **= ADJACENT CLUSTER TABLE CPNAME ENTRIES**
value represents the number of predefined or dynamic entries in the active adjacent cluster table. The adjacent cluster table is used by APPN Directory Services to select the sequence of nodes to search during border node search logic.

160 *value* **= CP-CP SESSIONS**
value represents the number of CP-CP sessions between this node and other nodes.

161 *value* **= HIGHEST ELEMENT ADDRESS ASSIGNED**
value represents the highest network address element number that has been assigned by VTAM. *value* is displayed in decimal. The maximum number of element addresses that can be assigned is 65 536 (X'0000' through X'FFFF').

162 *value* **= HIGHEST EXTENDED ELEMENT ADDRESS ASSIGNED**
value represents the highest extended network address element number that has been assigned by VTAM. *value* is displayed in decimal. The maximum number of element addresses that can be assigned is 16 777 216. See the ENHADDR start option information in z/OS Communications Server: SNA Resource Definition Reference for more information.

164 *value* **= NUMBER OF NON-EXTENDED ELEMENT ADDRESSES IN USE**
value represents the number of network element addresses currently in use by VTAM. value is displayed in decimal. The maximum number of element addresses that can be assigned is 65 536.

165 *value* **= NUMBER OF EXTENDED ELEMENT ADDRESSES IN USE**
value represents the number of extended network element addresses currently in use by VTAM. *value* is displayed in decimal. The maximum number of element addresses that can be assigned is 16 777 216. See the z/OS Communications Server: SNA Resource Definition Reference for more information.

170 *value* **= IDS3270 TOTAL SESSIONS MONITORED**
value represents the total number of sessions monitored by the 3270 Intrusion Detection Services. *value* is displayed in decimal.

171 *value* **= IDS3270 CURRENT SESSIONS MONITORED**
value represents the current number of sessions being monitored by the 3270 Intrusion Detection Services. *value* is displayed in decimal.

172 *value* **= IDS3270 SESSIONS MONITORED SINCE ENABLE**
value represents the total number of sessions monitored by the 3270 Intrusion Detection Services since the last time monitoring was enabled. *value* is displayed in decimal.

173 *value* **= IDS3270 TOTAL INCIDENTS FOUND**
value represents the total number of problems found by the 3270 Intrusion Detection Services. Message group IST2424I was issued to describe the problems. *value* is displayed in decimal.

174 *value* **= IDS3270 TOTAL SUPPRESSED CONSOLE REPORTS**
value represents the total number of times the 3270 Intrusion Detection Services suppressed the reporting of an incident by the IST2424I message group. However, a single message IST2424I is still written to the SYSLOG or console. *value* is displayed in decimal.

IST1315I

VTAM issues this message when the number of statistics to be displayed exceeds the value specified for the MAX or NUM operand.

keyword is either **MAX** or **NUM**.

number is the value specified for either the MAX or NUM operand.

IST1345I

This message is a header message for the information displayed in message IST1227I.

IST1349I

dddd-ddddd-ddd is the component identifier assigned by VTAM. This identifier is used by IBM for VTAM program maintenance.

See the explanation of opening and closing an application program in z/OS Communications Server: SNA Programming for a description of vector lists and more information about the component identifier.

IST1454I

count is the number of statistics displayed.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Routing code: 2

Descriptor code: 5

IST2424I 3270 DATA STREAM ERROR – netid.pluname netid.sluname

Explanation: This is the first of a group of messages that VTAM issues when a 3270 data stream error is found by the 3270 Intrusion Detection Services. A complete description of the message group follows.

```
 IST2424I 3270 DATA STREAM ERROR – netid.pluname netid.sluname
 IST2425I {PLU|SLU} SUBAREA = X'saHex' INDEX = X'indHex' ELEMENT =  X'elHex'
 IST2441I JOBNAME = jobname  SID = session_id
[IST2426I IPADDR = ipaddress..port]
 IST2427I DATE = date TIME = time ID = id
 IST2428I ROW = row COLUMN = col
 IST2429I OUTBOUND – SEQ = X'seq_num' OFF = offset LEN = len
 IST2431I hex_data1 hex_data2 hex_data3 hex_data4 *EBCDIC_data*
 IST2430I INBOUND  - SEQ = X'seq_num' OFF = offset LEN = len
 IST2431I hex_data1 hex_data2 hex_data3 hex_data4 *EBCDIC_data*
 IST314I END
```

IST2424I

pluname
: The network-qualified primary session partner name.

sluname The network-qualified secondary session partner name.

netid The ID of the network that contains the session partner.

IST2425I

IST2425I will be displayed once for the PLU resource and once for the SLU resource.

saHex The subarea of the primary or secondary logical unit in hexdecimal.

indHex The element index number of the primary or secondary logical unit in hexdecimal.

elHex The element address of the primary or secondary logical unit in hexdecimal.

IST2426I

ipaddress
: The IP address associated with the SLU.

port The port number associated with the SLU.

This message is issued when the control vector CV64 has been provided.

IST2427I

date **and** *time*
: Specify when the last outbound data was sent.

id The incident token associated with this event.

IST2428I

row The row number of the 3270 presentation space where the field modification was detected.

col The column number of the 3270 presentation space where the field modification was detected.

IST2429I

seq_num
The sequence number of the last outbound PIU that set the field in question in hexadecimal.

offset The offset in the outbound PIU of the field that was overlaid.

len The length of the outbound field that was overlaid.

IST2430I

seq_num
The sequence number of the inbound PIU in hexadecimal.

offset The offset in the inbound PIU of the field that was overlaid.

len The length of the inbound field that was overlaid.

IST2431I

hexdata_1, hex_data2, hex_data3 and hex_data4
Show up to 16 bytes of outbound or inbound data around the area of the detected violation (in hex).

EBCDIC_data
Show up to 16 bytes of outbound or inbound data around the area of the detected violation (in EBCDIC).

IST2441I

jobname The 1 to 8 character job name of the VTAM application that was active when the incident occurred. If *jobname* is not available, VTAM issues ***NA***.

session_id
The session ID that provides a unique identifier for the session. If the session ID is unknown, VTAM displays ***NA***.

System action: Depending on the value of the DSACTION defined on the APPL statement, the connection will be continued or will be terminated. The outbound and inbound PIUs have been written to the Generalized Trace Facility (GTF), if available.

Operator response: Notify the security administrator that a possible intrusion has been detected.

System programmer response: None.

User response: None.

Problem determination: Start the Generalized Trace Facility (GTF) to collect trace records of event type 'F90'x. These trace records can be formatted with Interactive Problem Control System (IPCS).

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 8, 9

Descriptor code: 4

Automation: An automation tool can start GTF and buffer trace for the SLU when it detects the message IST2424I.

Tips:

- When you use DSACTION=SYSLOG, a single IST2424I message is written to the console and the entire message group for IST2424I is written to SYSLOG. This message is displayed twice for the same incident during automation.
- When the application is TSO, the *jobname* in IST2441I is the TSO user ID.

Example:

```
IST2424I 3270 DATA STREAM ERROR - NETA.TSO10001 NETA.L7201A 056
IST2425I PLU SUBAREA = X'0001' INDEX = X'0001' ELEMENT = X'0076'
IST2425I SLU SUBAREA = X'0001' INDEX = X'0000' ELEMENT = X'003A'
IST2441I JOBNAME = USER1 SID = EAABEEC33D18556F
IST2426I IPADDR = 10.10.101.4..50208
IST2427I DATE = 2016/04/01 TIME = 14:07:04 ID = 1
IST2428I ROW = 4 COLUMN = 14
IST2429I OUTBOUND - SEQ = X'000A' OFF = 350 LEN = 66
IST2431I 00000000 00000000 00000000 00000000  *................*
IST2430I INBOUND - SEQ = X'0006' OFF = 6 LEN = 66
IST2431I 92939293 91A28400 00000000 00000000  *KLKLJSD.........*
IST314I END
```

IST2425I {PLU|SLU} SUBAREA = X'saHex' INDEX = X'indHex' ELEMENT = X'elHex'

Explanation: VTAM issues this message as part of a group of messages. The first message of the group is IST2424I. See the explanation of that message for a complete description. IST2424I is issued when a 3270 data stream error is detected.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 8, 9

Descriptor code: 4

IST2426I IPADDR = ipaddress..port

Explanation: VTAM issues this message as part of a group of messages. The first message of the group is IST2424I. See the explanation of that message for a complete description. IST2424I is issued when a 3270 data stream error is detected.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 8, 9

Descriptor code: 4

IST2427I DATE = *date* TIME = *time* ID = *id*

Explanation: VTAM issues this message as part of a group of messages. The first message of the group is IST2424I. See the explanation of that message for a complete description. IST2424I is issued when a 3270 data stream error is detected.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 8, 9

Descriptor code: 4

IST2428I ROW = row COLUMN = col

Explanation: VTAM issues this message as part of a group of messages. The first message of the group is IST2424I. See the explanation of that message for a complete description. IST2424I is issued when a 3270 data stream error is detected.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 8, 9

Descriptor code: 4

IST2429I OUTBOUND – SEQ = *X'seq_num'* **OFF =** *offset* **LEN =** *len*

Explanation: VTAM issues this message as part of a group of messages. The first message of the group is IST2424I. See the explanation of that message for a complete description. IST2424I is issued when a 3270 data stream error is detected.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 8, 9

Descriptor code: 4

IST2430I INBOUND - SEQ = *X'seq_num'* **OFF =** *offset* **LEN =** *len*

Explanation: VTAM issues this message as part of a group of messages. The first message of the group is IST2424I. See the explanation of that message for a complete description. IST2424I is issued when a 3270 data stream error is detected.

System action: None.

Operator response: None.

System programmer response: None.

User response: None.

Problem determination: Not applicable.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 8, 9

Descriptor code: 4

Automation: Not applicable for automation.

IST2431I hex_data1 hex_data2 hex_data3 hex_data4 *EBCDIC_data*

Explanation: VTAM issues this message as part of a group of messages. The first message of the group is IST2424I. See the explanation of that message for a complete description. IST2424I is issued when a 3270 data stream error is detected.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 8, 9

Descriptor code: 4

IST2432I 3270 ERROR SUMMARY FROM *date* AT *time*

Explanation: VTAM issues this message as part of a 3270 Intrusion Detection Services summary message group. This message group is issued only if message suppression has been enabled by setting the *error_msg_count* DSACTION start option to a nonzero value. VTAM suppresses the logging of the IST2424I message events if the number of message events logged in a 60-second interval exceeds the value of the DSACTION start option. Logging resumes after the 60-second interval ends. Message IST2439I is a column header for IST2440I, which is repeated for each session. The full description of the message group follows the example.

```
IST2432I 3270 ERROR SUMMARY FROM date AT time
IST2438I SESSIONS = sesscnt ERRORS = errcnt
IST924I -------------------------------------------------------------
IST2439I PLU              SLU              SID             ERRORS
[IST2440I pluname           sluname           sessionid         count]
.
.
.
IST314I END
```

IST2432I

In the message text:

date **and** *time*
Specify when the message suppression event interval was started. This summary message group displays information about messages that were suppressed since this date and time.

IST2438I

In the message text:

sesscnt The number of sessions recorded in the summary. This does not include sessions that could not be saved in the summary table. If *sesscnt* displays > 50, more than 50 sessions were associated with the IST2424I message groups.

errcnt The total number of errors that have occurred since message group IST2424I was suppressed. This does include the sessions that could not be saved in the summary table.

IST924I

VTAM issues this message to improve the readability of the display.

IST2439I

This message is a message header for the information displayed in message IST2440I.

IST2440I

In the message text:

pluname
The network-qualified primary session partner name.

sluname The network-qualified secondary session partner name.

sessionid
The session identifier. For additional information on the session, enter a DISPLAY SESSIONS,SID=*sessionid* command.

count The number of IST2424I message groups that was suppressed for the session.

If the *pluname* and *sluname* values contain N/A, this is the overflow entry and the *count* value contains the number of incidents that could not be recorded in the summary table.

System action: Processing continues. PIUs that are associated with the event are still written to GTRACE.

Operator response: Notify the security administrator that possible intrusions have been detected.

System programmer response: None.

User response: None.

Problem determination: Start the Generalized Trace Facility (GTF) to collect trace records of event type 'F90'x. These trace records can be formatted with Interactive Problem Control System (IPCS).

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 8, 9

Descriptor code: 4

Automation: An automation tool can start GTF and buffer trace for the secondary logical unions when it detects the message IST2432I.

Example:

```
IST2432I 3270 ERROR SUMMARY FROM 2016/01/07 AT 09:19:17 976
IST2438I SESSIONS = 1 ERRORS = 25
IST924I -------------------------------------------------------------
IST2439I PLU               SLU               SID             ERRORS
IST2440I NETA.TSO10001     NETA.L7201A       EAABEEC32FB66595    25
IST314I END
```

IST2433I DSMONITR = YES, DSCOUNT = *count*, **DSACTION =** *string*

Explanation: VTAM issues this message in response to a DISPLAY ID command for a VTAM application when the 3270 Intrusion Detection Services is active for this application.

In the message text:

count The number of outbound buffers to be saved. *count* is the current value of the DSCOUNT operand specified on the APPL statement or the VTAM DSCOUNT start option.

string The current value of the DSACTION operand specified on the APPL statement or the VTAM DSACTION start option.

System action: Processing continues.

Operator response: None.

System programmer response: None.

User response: Not applicable.

Problem determination: Not applicable.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 2

Descriptor code: 5

Automation: Not applicable for automation.

Example:

```
IST2433I DSMONITR = YES, DSCOUNT = 1, DSACTION = (SYSLOG,NONE)
```

IST2434I DSTRUST = *string*

Explanation: VTAM issues this message in response to a DISPLAY ID command for a VTAM application when the 3270 Intrusion Detection Services is active for this application.

In the message text:

string The current value of the DSTRUST operand specified on the APPL statement or the VTAM DSTRUST start option.

System action: Processing continues.

Operator response: None.

System programmer response: None.

User response: Not applicable.

Problem determination: Not applicable.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 2

Descriptor code: 5

Automation: Not applicable for automation.

Example:

```
IST2434I DSTRUST = NONE
```

IST2435I SESSIONS MONITORED = *count*, **ERRORS DETECTED =** *errors*

Explanation: VTAM issues this message in response to a DISPLAY ID command for an application program when the 3270 Intrusion Detection Services is monitoring this application.

In the message text:

count The number of sessions currently being monitored by the 3270 Intrusion Detection Services. When the 3270 Intrusion Detection Services is no longer actively monitoring sessions, ***N/A*** is displayed.

errors The number of errors that have been found by the 3270 Intrusion Detection Services for this application.

System action: Processing continues.

Operator response: None.

System programmer response: None.

User response: Not applicable.

Problem determination: Not applicable.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 2

Descriptor code: 5

Automation: Not applicable for automation.

IST2436I DSMONITR = NO

Explanation: VTAM issues this message in response to the following commands:

- DISPLAY ID command for an application program when the 3270 Intrusion Detection Services is not active for the application.
- DISPLAY SESSIONS,SID= command for a session when the 3270 Intrusion Detection Services is not active for the session.

System action: Processing continues.

Operator response: None.

System programmer response: Not applicable.

User response: Not applicable.

Problem determination: None.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 2

Descriptor code: 5

Automation: Not applicable for automation.

Example:

```
IST2436I DSMONITR = NO
```

IST2437I DSMONITR = [YES|NO], ERRORS DETECTED = *errors*

Explanation: This message is part of a group of messages that VTAM issues in response to a DISPLAY SESSIONS,SID command. The first message of the group is IST879I. See the explanation of that message for a complete description.

System action: Processing continues.

Operator response: None.

System programmer response: None.

User response: Not applicable.

Problem determination: Not applicable.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 2

Descriptor code: 5

Automation: Not applicable for automation.

Example:

```
IST2437I DSMONITR = YES, ERRORS DETECTED = 0
```

IST2438I SESSIONS = *sesscnt* **ERRORS =** *errcnt*

Explanation: VTAM issues this message as part of a 3270 Intrusion Detection Services summary message group. This message group is issued only if message suppression has been enabled by setting the *error_msg_count* DSACTION start option to a nonzero value. The first message in this message group is IST2432I. See the explanation of that message for a complete description.

System action: Processing continues.

Operator response: Notify the security administrator that possible intrusions have been detected.

System programmer response: None.

User response: None.

Problem determination: Start the Generalized Trace Facility (GTF) to collect trace records of event type 'F90'x. These trace records can be formatted with Interactive Problem Control System (IPCS).

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 8, 9

Descriptor code: 4

Automation: An automation tool can start GTF and buffer trace for the SLU when it detects the message IST2424I or IST2432I.

IST2439I PLU SLU SID ERRORS

Explanation: VTAM issues this message as part of a 3270 Intrusion Detection Services summary message group. This message group is issued only if message suppression has been enabled by setting the *error_msg_count* DSACTION start option to a nonzero value. The first message in this message group is IST2432I. See the explanation of that message for a complete description.

System action: Processing continues.

Operator response: Notify the security administrator that possible intrusions have been detected.

System programmer response: None.

User response: None.

Problem determination: Start the Generalized Trace Facility (GTF) to collect trace records of event type 'F90'x. These trace records can be formatted with Interactive Problem Control System (IPCS).

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 8, 9

Descriptor code: 4

Automation: An automation tool can start GTF and buffer trace for the SLU when it detects the message IST2424I or IST2432I.

IST2440I *pluname sluname sessionid count*

Explanation: VTAM issues this message as part of a 3270 Intrusion Detection Services summary message group. This message group is issued only if message suppression has been enabled by setting the *error_msg_count* DSACTION start option to a nonzero value. The first message in this message group is IST2432I. See the explanation of that message for a complete description.

System action: Processing continues.

Operator response: Notify the security administrator that possible intrusions have been detected.

System programmer response: None.

User response: None.

Problem determination: Start the Generalized Trace Facility (GTF) to collect trace records of event type 'F90'x. These trace records can be formatted with Interactive Problem Control System (IPCS).

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 8, 9

Descriptor code: 4

Automation: An automation tool can start GTF and buffer trace for the SLU when it detects the message IST2424I or IST2432I.

IST2441I **JOBNAME =** *jobname* **SID =** *session_id*

Explanation: VTAM issues this message as part of a group of messages. The first message of the group is IST2424I. See the explanation of that message for a complete description. IST2424I is issued when a 3270 data stream error is detected.

Source: z/OS Communications Server SNA

Module: Use the modifiable VTAM start option MSGMOD=YES (*f procname,vtamopts,msgmod*=yes or *f procname,msgmod*=yes) to display the issuing module when a message is issued. See z/OS Communications Server: SNA Operation and z/OS Communications Server: SNA Resource Definition Reference for more information about start options.

Routing code: 8, 9

Descriptor code: 4

Chapter 7. SNA Network Implementation Guide

Security features

VTAM provides a variety of security features that can be enabled for an application program, including:

- Cryptography facility
- Message authentication
- SLU authentication
- VTAM application security
- Confidential data
- 3270 Intrusion Detection Services

For information about LU 6.2 security features, see LU 6.2 security.

3270 Intrusion Detection Services

You can configure and monitor the VTAM 3270 Intrusion Detection Services (IDS) to determine problems in application 3270 data streams. The specific problem that is detected is the modification of protected fields in the data stream that 3270 emulators return.

This topic includes the following information:

- "3270 IDS overview" introduces the overview and background of the VTAM 3270 IDS function.
- "3270 IDS considerations and assessment" on page 65 describes the various factors to consider before deploying the 3270 IDS solutions, including assessing your environment, deployment strategy, and known application 3270 solutions provided by IBM.
- "Configuring 3270 IDS" on page 72 describes how to configure the monitoring of the 3270 data streams.
- "Displaying and modifying 3270 IDS configuration" on page 74 describes the configuration and status of 3270 IDS.
- "3270 IDS incidents" on page 77 describes the messages when 3270 data stream errors are detected.
- "GTF trace data" on page 78 describes how to capture and format 3270 IDS incident trace data when 3270 IDS incidents are written to the GTF.
- "Using SMF" on page 81 describes how to capture 3270 IDS incident trace data when 3270 IDS incidents are written to the SMF.
- "Incident validation" on page 81 describes methods for gathering information about incidents.

3270 IDS overview

The z/OS Communications Server VTAM 3270 Intrusion Detection Services (IDS) function can help alert you to 3270 protocol violations as they occur in real time. This can be useful in identifying potential intrusions that attempt to manipulate 3270 protocol flows with the goal of compromising 3270 SNA applications and data that are deployed on your z/OS systems. This function can detect, in real time, an attempt by a malicious 3270 client emulator to modify protected fields on a 3270 screen. By modifying protected fields, the malicious 3270 client emulator might be trying to subvert the normal processing of the 3270 server application.

The effect of such an attempt depends on how well the application guards itself against unexpected changes to protected fields. In the best case scenario, a modification to a protected part of the screen is ignored by the application. In the worst case scenario, it could cause a potentially harmful change in the application's behavior.

Well behaved 3270 client emulator software typically prevents users from entering input into protected parts of the screen. The concern is over malicious users that use 3270 client emulators that do not honor the 3270 protocol and allow changes to protected fields. The 3270 IDS function can detect these types of protocol violations. However, note that SNA 3270 protocol violations might occur without malicious intent. This might be the result of race conditions or lax adherence of the SNA 3270 protocol by software such as 3270 client software emulators, the TN3270 client, session managers, or other SNA based 3270 protocol software. These anomalies might even occur with a regular frequency in your environment and most often go unnoticed as they do not have an impact that is visible to administrators, applications, or users. In some cases, they might cause a temporary error condition on the 3270 client's screen that they can easily recover from. While the 3270 IDS function can flag all detected protocol violations, it cannot determine whether a protocol violation is a malicious attack or an inadvertent anomaly in the 3270 protocol. Additionally, it cannot provide any insight on how a server-side 3270 application deals with these protocol anomalies. In other words, it cannot detect whether an application is vulnerable to a 3270 protocol-based attack or not. The 3270 IDS function simply detects and notifies system administrators of the presence of protocol anomalies, which can be useful as an audit log of potentially suspicious events. In addition to notification, the 3270 IDS function can be configured to take action on the SNA session when a protocol violation is detected, such as terminating the session.

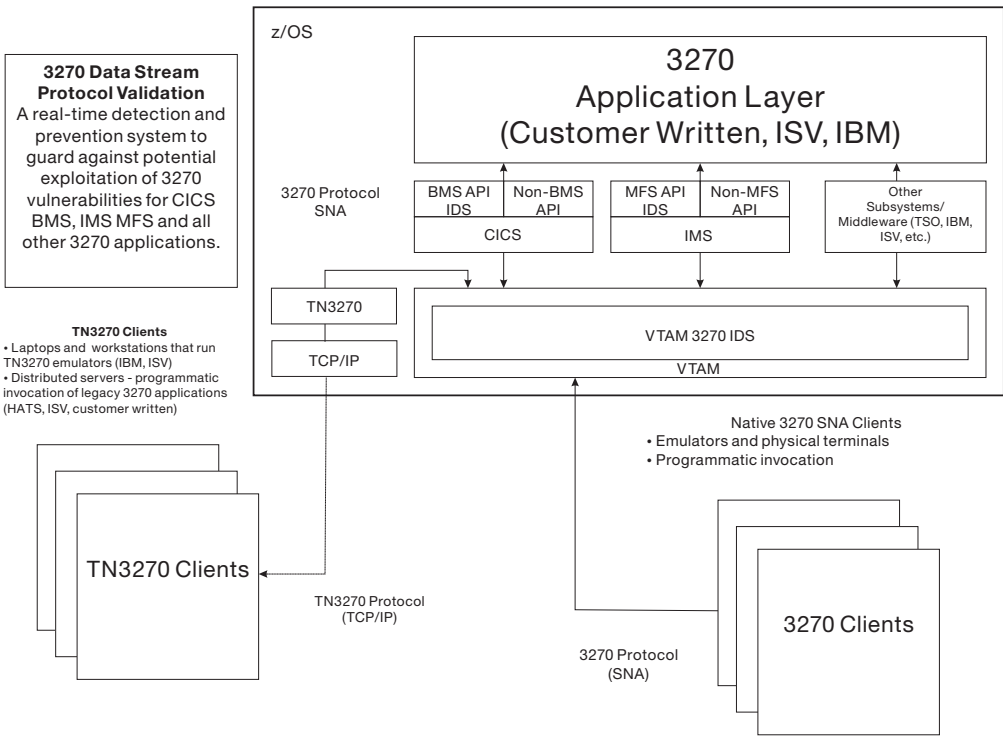


Figure 1. 3270 IDS protection overview

Note: The z/OS Communications Server VTAM 3270 IDS solution is one of several solutions that can provide detection and protection from malicious 3270 attacks.

Figure 1 on page 64 provides an overview of the following 3270 data stream protocol validation solutions:

CICS basic mapping support (BMS)
CICS provides 3270 IDS detection and protection for any applications that exploit CICS basic mapping support (BMS) interfaces to create and parse their 3270 screens. When this support is activated, CICS monitors the 3270 data streams to detect any attempted modifications to protected fields on the screen. CICS can then provide warnings (log and error message) or prevent the application from processing the data by abending the transaction. See the CICS product documentation through the IBM Knowledge Center: https://www.ibm.com/support/knowledgecenter/ for more information on the CICS BMS IDS solution.

IMS Message Formatting Service (MFS) support
Similar to the CICS BMS, IMS provides 3270 IDS support for any IMS applications that use the IMS Message Format Service (MFS) to format and parse their 3270 messages. When this function is enabled, IMS prevents modifications to protected fields from being passed on to IMS server applications. See the IMS product documentation through the IBM Knowledge Center: https://www.ibm.com/support/knowledgecenter/ for more information on the IMS MFS IDS solution.

VTAM 3270 IDS support
The VTAM 3270 IDS support is described in this topic.

ISPF also provides built-in IDS support. ISPF is one of the other subsystems shown in Figure 1 on page 64. Applications that use ISPF services to display their 3270 panels are automatically protected by ISPF. ISPF automatically detects and prevents any modifications to protected areas of the panels from occurring.

The list of 3270 data stream protocol validation solutions is not intended to be an exhaustive list. The other subsystems or other middleware category shown in Figure 1 on page 64 is intended to indicate any other potential application layer 3270 IDS support that might exist but is not identified here.

Note:

- The 3270 client emulators that are used by the 3270 users can use native SNA attachment directly to VTAM or IP attachment through TN3270. The VTAM and middleware 3270 IDS support that is shown in Figure 1 on page 64 covers all 3270 users.
- The terminology in this topic refers to general 3270 validation support, which is different from the specific terminology, such as CICS BMS, IMS MFS, or VTAM 3270 IDS, which refers to validation support within specific products that support the 3270 protocol.

3270 IDS considerations and assessment

This topic describes the various factors that you should consider, steps for assessing your exposure to potential 3270 protocol-based attacks, and your potential need for deploying one or more of the 3270 IDS solutions that are described in "3270 IDS overview" on page 63.

Assessing your environment:

If you have workloads that are protected by middleware or native application 3270 validation, evaluate the solutions that are described in "3270 IDS overview" on page 63 first before you investigate the z/OS Communications Server VTAM 3270 IDS function. Generally, the application solutions have a much lower overhead for IDS processing than the z/OS Communications Server VTAM solution, as they already have existing processing for the processing and handling the 3270 data streams.

The z/OS Communications Server VTAM 3270 IDS function can complement these solutions if you have workloads that you determine are at risk and are not covered by other IDS solutions. As a result, the z/OS Communications Server VTAM 3270 IDS solution is not necessarily required by all z/OS systems or users who have SNA 3270 application workloads. As with any intrusion detection capabilities, you must take careful considerations before you enable a 3270 IDS function. For this reason, the background information is provided here for you to analyze and determine whether this type of IDS function can provide value to your environment. As part of this analysis, you need to understand the z/OS Communications Server VTAM 3270 IDS function, other 3270 IDS options and applicability to your environment, and then assess the risk and cost factors in your environment.

This topic provides information to assist you in your assessment for the potential need of this function in your z/OS environment by evaluating the following aspects:

Applications
: Identify candidate applications and perform a careful analysis of need. See SNA application applicability criteria.

End users, SNA technology and connectivity
: Evaluate the users, key SNA technologies, and network configuration considerations. See exploitation factors and their implications in "SNA technologies, network connectivity, and environmental factors" on page 69.

Exploitation cost
: Understand the cost to exploit this function. See system resource cost and administrative considerations in Exploitation cost.

Complete this assessment carefully, and then consider moving forward with the exploitation of the 3270 IDS function.

SNA application applicability criteria
Is the 3270 IDS function needed in your environment?:
Many factors help determine the need for the validation protection that is provided by the 3270 IDS function. To make this assessment, you need background in securing SNA workloads. See the 3270 Emulation: Security Considerations white paper for initial information.

After reviewing the security information in this white paper, you can continue your assessment by using the following key 3270 IDS considerations.

Carefully evaluate your SNA applications for each z/OS system. This topic provides considerations for your SNA application workloads (per z/OS system).

SNA applications

All z/OS systems have 3270 application workloads. At a minimum, the system administrators use various TSO/ISPF functions to maintain z/OS and often to

manage other applications. Beyond the system administrators, various applications can exploit SNA APIs that are related to SNA LU0 and LU2 3270 workloads. The first step in your assessment is to identify all of the 3270 applications on your applicable z/OS systems. To assist with this step, use the VTAM operator display command **D NET,APPLS,SCOPE=3270CAND**. This display provides the following information:

3270 candidate applications
: Displays a list of active VTAM applications that have any LU-LU sessions (since the ACB was opened) that qualify for the 3270 IDS monitoring. The qualifying LU sessions must be LU type LU0 with TS profile 2 or LU2 with TS profile 3. Applications that have qualifying LU sessions are potential candidates for the 3270 IDS function.

LU session count
: A cumulative session count (since the ACB was opened) of the number of qualifying LU sessions.

While all applications in this list are candidates, you should initially focus on the applications with the highest qualified LU session counts. After you identify your candidate 3270 applications, you need to evaluate the application 3270 support for each of those applications.

After you identify the applications to focus on, consider whether the VTAM 3270 applications themselves or the middleware under which they run, for example, IBM middleware such as CICS or IMS, offer any native 3270 protocol related validation or protection. As described in "3270 IDS overview" on page 63, CICS and IMS provide modes (BMS and MFS) for their applications to exploit 3270 communications that also provide 3270 protocol validation. You should first evaluate the data validation support that is provided by the IBM middleware and possibly by the application programs themselves. You might need to consult with the CICS or IMS application programming staff to understand what modes are exploited. If the VTAM 3270 application does not run under a middleware environment that provides its own 3270 IDS function, you need to consult with the application support staff or supporting documentation for the application.

If protocol validation is offered by the middleware or application, enable its support. The 3270 middleware or application is typically in a better position to perform this type of protocol validation. With an existing understanding of the 3270 data stream context, middleware and application validation is typically much more efficient than the VTAM IDS approach. The application can also provide for some error recovery, retries, or have the capability to ignore certain anomalies or error conditions.

Figure 2 on page 68 provides an overview of the candidate application assessment process. For each candidate 3270 application, start your assessment here.

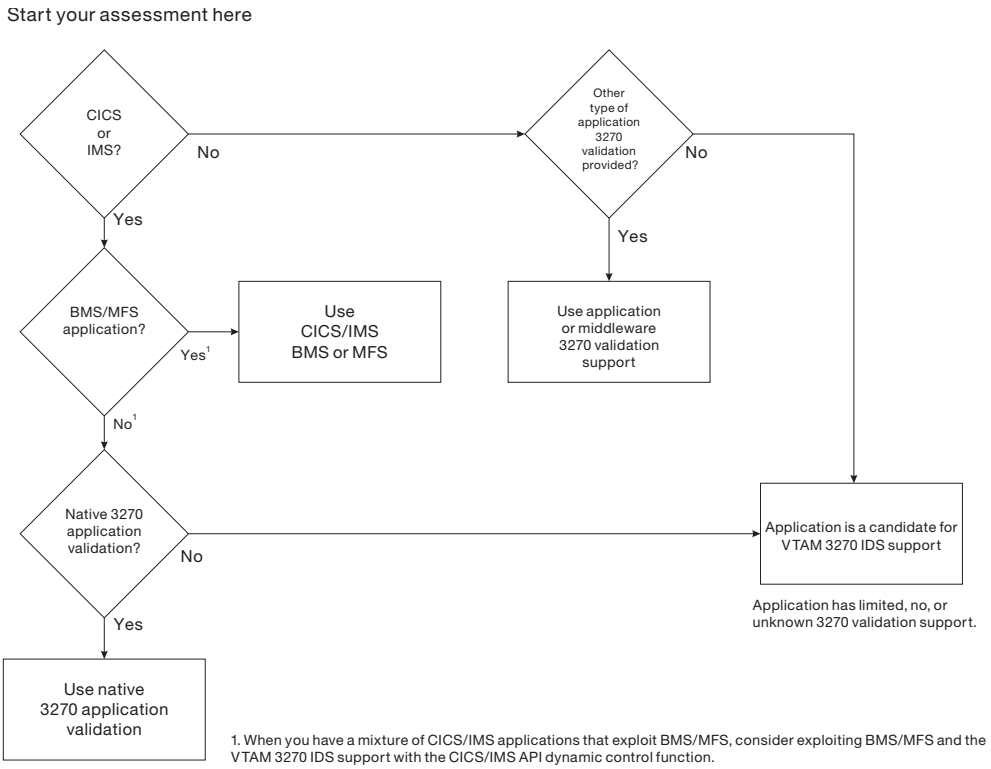


Figure 2. Candidate application assessment process

After you complete your assessment of the candidate applications and their native 3270 validation support, you might determine that the VTAM 3270 IDS validation is not required for your list of identified applications. If you do have a list of candidate applications without coverage or you have a list of potential candidate applications that have unknown validation capability, continue your assessment.

3270 user community of end users

For the identified candidate applications, how well do you understand the configuration and access of your 3270 emulators and the actual end users? For example, who are your end users for each application? Are the users internal or within your company, or are some of them external users? How many users are there?

For the users of each application, what forms of access control and authentication do you have in place for the 3270 users, for example, TLS/SSL, SAF-based, custom written, and so on?

More SNA related aspects are also end user considerations:

- Can you identify or inventory the various SNA components that are used for host access by this set of users?
- What is your level of control and confidence for the security of the following components:
  - TN3270 server products
  - TN3270 client products
  - What products do the SNA session managers support?

– Do the SNA native connections use TN3270 access? If yes, what 3270 access solutions are being used?

You might not need the 3270 validation for this application, if both the following conditions are met:

- The scope of your end users who have access to your 3270 applications is known and limited.
- The level of control or trust (authentication) you have with the access for those end users (including the control over and integrity of the TN3270 client software and protection it provides) is high.

Consider performing a risk assessment to determine whether the additional protection of an IDS solution is warranted for this application by considering this set of users and the client software used by the users. To complete this part of the assessment, you might need to consult with the 3270 client emulator vendor.

See "SNA technologies, network connectivity, and environmental factors" for more end user related considerations.

SNA technologies, network connectivity, and environmental factors:
Figure 3 illustrates a typical SNA 3270 network configuration that shows an SNA session manager and a TN3270 server that are located within the same z/OS instance. Several key environmental and configuration aspects are related to identifying and reporting 3270 protocol violations. Some aspects overlap with the previous end user considerations.

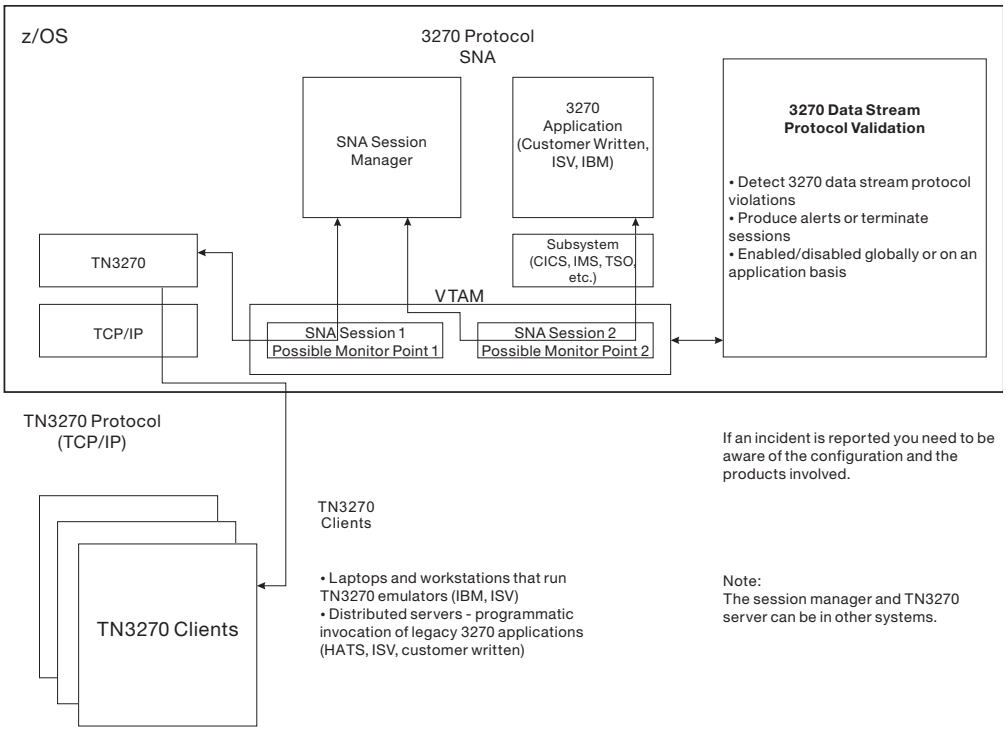


Figure 3. Sample of typical SNA 3270 network configuration

Many variables in an SNA 3270 network can impact the flow of the 3270 data stream. Among these are layers of SNA components, connectivity, and often SNA

session management products. The session flow can potentially have an impact on the 3270 protocol validation processing. Consider your unique environmental aspects, for example:

- Systems or network topology: CPU utilization/availability and network topology, network configuration, and network equipment, which can all impact latency that impacts timing.
- Your 3270 related products and vendors, for example, the 3270 application (IMS, CICS, and so on), the TN3270 servers, whether on z/OS or other platforms, the 3270 clients, possible SNA session managers, your end users, and native SNA connectivity when applicable.
- Product compliance, level and compatibility of the SNA LU0 and LU2 3270 protocols, each product in the path of the 3270 data stream, including the 3270 client emulator product, adherence to and implementation of the SNA LU0 and SNA LU2 3270 architecture (including any applicable SNA extensions).
- Your 3270 system and network configuration, physical proximity of resources and IP topology (relative to the 3270 application), the location of the session manager, the TN3270 server and platform, the 3270 client (distance and other network topology aspects) that can all impact timing.

If you have SNA session managers that run on your z/OS system as illustrated in Figure 3 on page 69, you should disable VTAM 3270 IDS for the traffic between the 3270 clients and the session managers to avoid double validation for the same 3270 data streams. Instead, only perform the validation between the session manager and the actual 3270 application.

It is important to understand that the VTAM 3270 IDS function reports any violation of the 3270 protocol that causes a protected field to be overwritten. The violation might be the result of malicious activity or the result of unintentional protocol anomalies (inadvertent or transient protocol violations that are caused by things like timing or queuing anomalies).

The VTAM 3270 IDS function cannot make the distinction between a malicious activity versus an unintentional protocol anomaly. Instead, such distinction requires careful analysis of the captured documentation that is associated with the reported incident. In many cases, this type of error can be handled (ignored or retried) by the application.

The frequency of reporting unintentional protocol anomalies varies for each environment. In some environments, the amount or frequency of reporting of unintentional protocol anomalies can be problematic. For each reported incident, you need to perform the initial evaluation to determine the disposition of the IDS incident. If the reported incident is a known unintentional protocol anomaly, that type of incident can be self-managed. If the reported incident is determined to be a malicious attack, you can use the information that is recorded by the VTAM 3270 IDS function to begin your effort to identify the source of the attack. Finally, you might determine that the reported incident is a valid use of the 3270 protocol even though the VTAM 3270 IDS support flagged it. In that case, you might need to work with IBM service to determine the disposition of the incident.

Exploitation cost
System resource cost and other implications of exploitation:
Consider system resources (CPU and storage) and administrative costs that are related to the exploitation of the VTAM 3270 IDS function. The actual performance

impact of enabling the function varies for each customer environment depending on the scope of the support enabled the application workloads and the type of 3270 traffic.

Processing cost

Internal IBM benchmarks indicate that the IDS analysis that is performed by VTAM 3270 IDS function can result in an increase in CPU use for the SNA application address space, for example, the CICS TOR address space. The amount of increase is impacted by several factors such as the format, complexity, and size of the 3270 screens typically used by the application. The number of LU sessions is another key factor.

If you have SNA session managers that run on your z/OS system, you should disable VTAM 3270 IDS for the traffic between the 3270 clients and the session managers to avoid double validation for the same 3270 data streams. Instead, only perform the validation between the session manager and the actual 3270 application.

Virtual memory cost

Each SNA session that is enabled for the 3270 IDS function allocates approximately 100 K for the session and extra storage for outbound PIU tracking. The VTAM DSCOUNT start option determines how many outbound PIUs to save. The DSCOUNT setting along with PIU (screen) size directly affects the amount of virtual memory that is used to monitor the session. The session-related storage is all 64-bit virtual storage. Total virtual storage can be estimated by multiplying 125 K by total sessions monitored. You need to insure that enough real and virtual memory (paging space) is available before you enable this function on a system. Additionally, insure that system parameters such as MEMLIMIT are set to appropriate values that do not artificially limit the amount of 64-bit storage that is available to the relevant address spaces.

Administrative cost

Administrative costs are associated with your initial applicability analysis, enablement, and monitoring. Some coordination might be required with the applications administrative staff as well. After the VTAM 3270 IDS function is enabled, each reported incident provides diagnostic data that needs to be evaluated by your staff. This might include network administrators, application developers, other personnel who are familiar with the 3270 data streams in question. If your evaluation concludes that the incident does not reflect any type of protocol violation, you can contact IBM for further assistance.

In some cases, the exploitation of this IDS function might result in persistent and ongoing reporting of similar unintentional protocol anomalies; for example, due to specific vendor products such as TN3270 server, client emulation support, session managers. In such cases, you are required to work with the associated vendor product support staff for a resolution. Pending a resolution, the VTAM 3270 IDS function can be disabled for such workloads.

IBM provides changes for the z/OS TN3270 Telnet Server and the CS Distributed Telnet Server that are related to timing scenarios that can result in reporting of protocol anomalies. For more information about those issues and related changes, see the product support information for those products.

Deployment strategy:

After you complete the assessment for each z/OS system and the applicable application workloads on those systems and you believe that your environment can benefit from the VTAM 3270 IDS function, you should consider creating an exploitation plan that enables the support on your systems in a controlled and gradual manner in terms of systems and applications. The objective is to gradually extend the support to the various 3270 application workloads. For example, the support should start with test or development systems for specific applications. After the support is active for a period of time and you have assessed the impact, you can continue expanding the support to other workloads and systems.

Do not code the DSACTION=SENSE option that raises error condition to the z/OS 3270 application or the DSACTION=TERM option that terminates corresponding LU-LU session until you have sufficient experience with a workload and justification for this setting. While you expose more systems and workloads to this validation support, you can assess the impact to your environment and the effectiveness for your workloads.

Known application 3270 solutions provided by IBM: CICS and IMS application 3270 validation support

Both IMS and CICS products provide the following native 3270 validation support:

- CICS BMS data stream protection
- IMS MFS data stream protection

Both of these solutions require less processing and CPU than the VTAM 3270 IDS solution. For more information about the CICS or IMS support, see the CICS or IMS product documentation for related PTF or base product information.

Application API dynamic control

The VTAM IDS support also provides the capability for applications to dynamically control (enable/disable) the VTAM IDS validation function. With this support, middleware-based IDS solutions can temporarily disable the VTAM IDS function when the middleware IDS solution is actively protecting a session or avoiding dual monitoring of the session when both middleware and VTAM IDS solutions are active for a session. IBM middleware products, such as CICS, IMS, and ISPF, provide this support. For more information about the dynamic IDS exploitation provided by CICS or IMS, see the related product documentation.

TSO/ISPF considerations

TSO users, who are in the ISPF environment, are protected by the ISPF built-in 3270 validation support that is always active. Other TSO environments (non ISPF) need to be investigated and can be a candidate for the z/OS Communications Server VTAM 3270 IDS support. ISPF uses the application API dynamic control when processing ISPF panels.

Configuring 3270 IDS

About this task

To control the monitoring of 3270 data streams, you can use the following start options or specify the following parameters on the GROUP and APPL statements in an application major node.

DSMONITR
Controls the basic function of the monitoring.

DSACTION
Controls the actions that will be taken when an incident occurs.

DSCOUNT
Controls the number of outbound 3270 data streams to help reconstruct the events that cause the incident.

DSTRUST
Controls the type of secondary logical units that are trusted and therefore not monitored.

Procedure

Sample configuration on the ATCSTRDS, ATCCONDS, and TSO1A parameters shows the definitions that are required for the 3270 IDS monitor function. This sample configuration enables the following functions:

- Only the TSO applications are monitored.
- The local logical units are trusted, but others are not.
- Message group IST2424I is written to the console.
- No additional action will be taken when an incident is detected.
- If more than 10 incidents occur within 60 seconds, writing the message group IST2424I stops for the rest of those 60 seconds.
- Up to 15 outbound buffers are saved for each session that is monitored.

Perform the following steps to configure 3270 Intrusion Detection Services:

1. Configure the ATCSTRDS member with the DSMONITR keywords.

```
*********************************************************************
*                                                                   *
*  SAMPLE PARAMETER FOR THE 3270 INTRUCTION DETECTION SERVICES      *
*                                                                   *
*********************************************************************
 DSMONITR=APPL,               MONITOR ONLY APPLS WITH DSMONITR=YES
 DSACTION=(CONSOLE,NONE,10),  MESSAGES TO THE CONSOLE
 DSCOUNT=15,                  SAVE UP TO 15 OUTBOUND BUFFERS
 DSTRUST=NONE,                COLLECT FOR ALL TYPES OF SESSIONS
 CONFIG=DS,                   START CONFIG
...
Rest of the VTAM start member
```

2. Configure the VTAM member ATCCONDS to define the TSO application major node at start up.

```
*********************************************************************
*
*  NAME:  ATCCONDS
*
*  USE:   CONFIGURATION LIST FOR SSCP1A.
*
*
*  SECURITY: IBM INTERNAL USE ONLY
*********************************************************************
        TSO1A,                TSO Applications                    X
...
```

3. Configure the VTAM TSO application major node.

```
*********************************************************************
*
*  NAME:  TSO1A
*
*  USE:   APPL DECK FOR TSO
*
*********************************************************************
         VBUILD TYPE=APPL
         GROUP DSMONITR=YES,DSTRUST=LOCALLU
*********************************************************************
*  THE FOLLOWING APPLS ARE FOR TSO/VTAM
*********************************************************************
TSO1     APPL  ACBNAME=TSO,AUTH=(NOACQ,PASS,NVPACE,TSO,NOPO),EAS=1,    C
               DSMONITR=NO
TSO10001 APPL  ACBNAME=TSO0001,AUTH=(NOACQ,PASS,NVPACE,TSO,NOPO),EAS=1
TSO10002 APPL  ACBNAME=TSO0002,AUTH=(NOACQ,PASS,NVPACE,TSO,NOPO),EAS=1
TSO10003 APPL  ACBNAME=TSO0003,AUTH=(NOACQ,PASS,NVPACE,TSO,NOPO),EAS=1
TSO10004 APPL  ACBNAME=TSO0004,AUTH=(NOACQ,PASS,NVPACE,TSO,NOPO),EAS=1
TSO10005 APPL  ACBNAME=TSO0005,AUTH=(NOACQ,PASS,NVPACE,TSO,NOPO),EAS=1
TSO10006 APPL  ACBNAME=TSO0006,AUTH=(NOACQ,PASS,NVPACE,TSO,NOPO),EAS=1
TSO10007 APPL  ACBNAME=TSO0007,AUTH=(NOACQ,PASS,NVPACE,TSO,NOPO),EAS=1
TSO10008 APPL  ACBNAME=TSO0008,AUTH=(NOACQ,PASS,NVPACE,TSO,NOPO),EAS=1
TSO10009 APPL  ACBNAME=TSO0009,AUTH=(NOACQ,PASS,NVPACE,TSO,NOPO),EAS=1
TSO10010 APPL  ACBNAME=TSO0010,AUTH=(NOACQ,PASS,NVPACE,TSO,NOPO),EAS=1
```

In this sample definition, the GROUP DSMONITR value is set to YES, but the APPL DSMONITR definition for TSO1 is set to NO. Because TSO does a CLSDST PASS to the other TSO applications, no 3270 monitoring is needed for this application.

Displaying and modifying 3270 IDS configuration

You can use VTAM commands to display the status of 3270 monitoring or to change the 3270 monitoring configuration.

- Start VTAM. No messages are issued for the 3270 IDS function during VTAM start up.

```
S NET,,,(LIST=DS)
IEF403I NET - STARTED - TIME=09.58.50
IST1054I VALUE FOR SIZE MUST BE BETWEEN 4M AND 2048M
IST448I DSPSIZE OPTION IGNORED - NO LONGER SUPPORTED
IST093I ISTCDRDY ACTIVE
IST315I VTAM INTERNAL TRACE ACTIVE - MODE = INT, SIZE = 0004 MB
IST199I OPTIONS = API APPC CFS CIA CIO CMIP CSM ESC HPR LCS LOCK MSG
IST199I OPTIONS = NRM PIU PSS SMS SSCP TCP VCNS XBUF XCF
IST314I END
...
IST093I TSO1A ACTIVE
...
IST020I VTAM INITIALIZATION COMPLETE FOR CSV2R1
IST1349I COMPONENT ID IS 5695-11701-210
IST1348I VTAM STARTED AS INTERCHANGE NODE
```

- Issue the **Display NET,VTAMOPTS,FUNCTION=SECURITY** command to display the current values of the DSMONITR keywords.

```
DISPLAY NET,VTAMOPTS,FUNCTION=SECURITY
IST097I DISPLAY ACCEPTED
IST1188I VTAM CSV2R1 STARTED AT 09:58:50 ON 01/25/16 655
IST1349I COMPONENT ID IS 5695-11701-210
IST1348I VTAM STARTED AS INTERCHANGE NODE
IST1189I DSACTION = (CONSOLE,NONE,10)    DSCOUNT  = 15
IST1189I DSMONITR = APPL                 DSTRUST  = NONE
IST1189I ENCRPREF = NONE                 ENCRYPTN = 31
IST1189I IPINFO   = SENDALL              SECLVLCP = ***NA***
IST1189I VERIFYCP = NONE
IST314I END
```

- Issue the **MODIFY proc,DSMONITR=NO** command to turn off the DSMONITR function. The **MODIFY** command stops the 3270 IDS monitoring. When secondary logical units send or receive a 3270 data stream, monitoring for the session is stopped. If the value of the DSMONITR keyword is changed back to YES, monitoring starts when a secondary logical unit starts a new session with the application.

```
MODIFY NET,VTAMOPTS,DSMONITR=NO
IST097I MODIFY ACCEPTED
IST223I MODIFY COMMAND COMPLETED
```

- Issue the **Display VTAMOPTS** command to display the updated values.

```
D NET,VTAMOPTS,FUNCTION=SECURITY
IST097I DISPLAY ACCEPTED
IST1188I VTAM CSV2R1 STARTED AT 09:58:50 ON 01/25/16 946
IST1349I COMPONENT ID IS 5695-11701-210
IST1348I VTAM STARTED AS INTERCHANGE NODE
IST1189I DSACTION = (CONSOLE,NONE,10)    DSCOUNT  = 15
IST1189I DSMONITR = NO                   DSTRUST  = NONE
IST1189I ENCRPREF = NONE                 ENCRYPTN = 31
IST1189I IPINFO   = SENDALL              SECLVLCP = ***NA***
IST1189I VERIFYCP = NONE
IST314I END
```

- Issue the **Display NET,ID=***applname* command to display the status of an application. The status of ACTIV/3-S indicates that this session is being monitored.

```
D NET,ID=TSO0002,SCOPE=ALL
IST097I DISPLAY ACCEPTED
IST075I NAME = TSO0002, TYPE = APPL 986
IST486I STATUS= ACT/S, DESIRED STATE= ACTIV
IST1447I REGISTRATION TYPE = NO
IST599I REAL NAME = NETA.TSO100021
IST977I MDLTAB=***NA*** ASLTAB=***NA***
IST861I MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I DLOGMOD=***NA*** USS LANGTAB=***NA***
IST1632I VPACING =  7
IST1938I APPC = NO
IST597I CAPABILITY-PLU ENABLED  ,SLU DISABLED ,SESSION LIMIT NONE
IST231I APPL MAJOR NODE = TSO1A
IST213I ACBNAME FOR ID = TSO10001
IST654I I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I STATE TRACE = OFF
IST271I JOBNAME = JHACKER, STEPNAME = OS390R5, DSPNAME = ISTFF999
IST228I ENCRYPTION = OPTIONAL , TYPE = DES
IST1563I CKEYNAME = TSO10001 CKEY = PRIMARY CERTIFY = NO
IST1552I MAC = NONE MACTYPE = NONE
IST1050I MAXIMUM COMPRESSION LEVEL - INPUT = 0, OUTPUT = 0
IST1633I ASRCVLM = 1000000
IST1634I DATA SPACE USAGE: CURRENT = 0 MAXIMUM = 0
IST2433I DSMONITR = YES, DSCOUNT = 15, DSACTION = (CONSOLE,NONE)
IST2434I DSTRUST = LOCALLU
IST2435I SESSIONS MONITORED = 1, ERRORS DETECTED = 0
IST171I ACTIVE SESSIONS = 0000000001, SESSION REQUESTS = 0000000000
IST206I SESSIONS:
IST634I NAME     STATUS         SID          SEND RECV VR TP NETID
IST635I TCPM0001   ACTIV/3-S   EAABEEC331E8DB02 0016 0003       NETA
IST314I END
```

- Issue the **D NET,SESSIONS** command to display information about the session. Message IST2436I or IST2437I shows the status of the 3270 IDS monitor.

```
D NET,SESSIONS,SID= EAABEEC331E8DB02
IST097I DISPLAY ACCEPTED
IST350I DISPLAY TYPE = SESSIONS 056
IST879I PLU/DLU REAL = NETA.TSO10001     ALIAS = NETA.TSO0002
IST879I SLU/OLU REAL = NETA.L7201A       ALIAS = ***NA***
IST880I SETUP STATUS = ACTIV/3
IST933I LOGMODE=D4B32XX3, COS=*BLANK*
IST1635I PLU HSCB TYPE: FMCB LOCATED AT ADDRESS X'176F5188'
IST1635I SLU HSCB TYPE: LUST LOCATED AT ADDRESS X'175A9314'
IST2437I DSMONITR = YES, ERRORS DETECTED = 0
IST2064I PLU TO SLU RU SIZE = 65535    SLU TO PLU RU SIZE =  6144
IST1636I PACING STAGE(S) AND VALUES:
IST1637I PLU--STAGE 1--SLU
IST1638I STAGE1: PRIMARY TO SECONDARY DIRECTION - FIXED
IST1639I         PRIMARY SEND: CURRENT   =     0     NEXT =     0
IST1640I         SECONDARY RECEIVE       =     0
IST1641I STAGE1: SECONDARY TO PRIMARY DIRECTION - NO PACING
IST1714I NO PATH INFORMATION EXISTS
IST314I END
```

- Issue the **D NET,STATS,TYPE=VTAM** command to display statistics about IDS activity.

```
D NET,STATS,TYPE=VTAM
IST097I DISPLAY ACCEPTED
IST350I DISPLAY TYPE = STATS,TYPE=VTAM 308
IST1349I COMPONENT ID IS 5695-11701-210
IST1345I    ID      VALUE        DESCRIPTION
IST1227I   151          0 = DEPENDENT LU TOTAL FOR ISTPUS
IST1227I    11          0 = CHANNEL-TO-CHANNEL ATTACHMENTS
IST1227I    61          0 = SNA DATA COMPRESSION SESSIONS
IST1227I    63         24 = RECOVERABLE SESSIONS
...
IST1227I   170          1 = IDS3270 TOTAL SESSIONS MONITORED
IST1227I   171          1 = IDS3270 CURRENT SESSIONS MONITORED
IST1227I   172          1 = IDS3270 SESSIONS MONITORED SINCE ENABLE
IST1227I   173          0 = IDS3270 TOTAL INCIDENTS FOUND
IST1227I   174          0 = IDS3270 TOTAL SUPPRESSED CONSOLE REPORTS
IST1454I 91 STATISTICS DISPLAYED
```

- Display the status of CSM storage.

  Tip: If too much HVCOMM storage is in use, consider reducing the DSCOUNT value.

```
D NET,CSM
IVT5508I DISPLAY ACCEPTED
IVT5529I PROCESSING DISPLAY CSM COMMAND - OWNERID NOT SPECIFIED
IVT5530I BUFFER BUFFER
IVT5531I SIZE   SOURCE                INUSE      FREE     TOTAL
IVT5532I ------------------------------------------------------
...
IVT5532I ------------------------------------------------------
IVT5533I    4K  HVCOMM                   4K     1020K        1M
IVT5533I   16K  HVCOMM                   0M        0M        0M
IVT5533I   32K  HVCOMM                  32K      992K        1M
IVT5533I   60K  HVCOMM                 120K      900K     1020K
IVT5533I  180K  HVCOMM                   0M        0M        0M
IVT5535I TOTAL  HVCOMM                 156K     2912K     3068K
...
IVT5604I HVCOMM MAXIMUM =     2000M  HVCOMM CURRENT =        3M
IVT5541I HVCOMM MAXIMUM USED =        3M SINCE LAST DISPLAY CSM
IVT5594I HVCOMM MAXIMUM USED =        3M SINCE IPL
...
IVT5599I END
```

3270 IDS incidents

If the 3270 IDS monitor detects a 3270 data stream error, an incident report is issued.

```
IST2424I 3270 DATA STREAM ERROR - NETA.TSO0002 NETA.TCPM0001
IST2425I PLU SUBAREA = X'0001' INDEX = X'0001' ELEMENT = X'0076'
IST2425I SLU SUBAREA = X'0001' INDEX = X'0000' ELEMENT = X'003A'
IST2441I JOBNAME = JHACKER SID = EAABEEC331E8DB02
IST2426I IPADDR = 192.168.98.254..61691
IST2427I DATE = 2016/01/25 TIME = 15:47:56 ID = 1
IST2428I ROW = 9 COLUMN = 16
IST2429I OUTBOUND - SEQ = X'0001' OFF = 598 LEN = 39
IST2431I 40404040 40404040 D1C1C3D2 E2D6D540  *        JACKSON *
IST2430I INBOUND - SEQ = X'0001' OFF = 284 LEN = 39
IST2431I 40404040 40404040 F1F2F3F4 F5F6F7F8  *        12345678*
IST314I END
```

Messages IST2424I, IST2425I, IST2441I, IST2426I, and IST2427I describe the identifying information about the incident. Messages IST2428I, IST2429I, IST2430I, and IST2431I describe the information about the specific data that caused the incident. This same information is written to the Generalized Trace Facility (GTF) by using the Event ID (EID) value x'F90'.

Use automation to start GTF when message IST2430I is issued in case any additional incidents exist. It is recommended that you have GTF running before the message IST2430I is issued to avoid the need for a recreate. In addition, VTAM buffer trace can be started for the secondary logical unit.

Tip: If the DSACTION=SYSLOG option is active, an IST2424I message is written to the console and the IST2424I message group is written to SYSLOG. The IST2424I message appears twice for the same incident in the automation program.

If the number of incidents that occur in a 60-second interval is more than the *msg-count* parameter of the DSACTION start option, the IST2424I message groups are not displayed on the console. When the interval expires, the message group IST2432I is displayed on the console.

```
IST2432I 3270 ERROR SUMMARY FROM 2016/01/25 AT 15:49:34
IST2438I SESSIONS = 1 ERRORS = 3
IST924I -------------------------------------------------------------
IST2439I PLU               SLU               SID             ERRORS
IST2440I NETA.TSO10002     NETA.TCPM0001     EAABEEC331E8DB02     3
IST314I END
```

Use the **CSDUMP** or **SLIP** command to capture a dump when an incident occurs.

Example when you use the **CSDUMP** command.

```
F NET,CSDUMP,MESSAGE=IST2430I
IST097I MODIFY ACCEPTED
IST223I MODIFY CSDUMP COMMAND COMPLETED
D NET,CSDUMP
IST097I DISPLAY ACCEPTED
IST350I DISPLAY TYPE = CSDUMP TRIGGERS 993
IST1871I MESSAGE TRIGGER: MESSAGE = IST2430I MATCHLIM = 1
IST1875I SENSE TRIGGER: NONE
IST314I END
...
IEA045I AN SVC DUMP HAS STARTED AT TIME=13.37.09 DATE=02/08/2016 046
FOR ASIDS(0031,001D)
QUIESCE = YES
IST1879I VTAM DUMPING FOR CSDUMP TRIGGER MESSAGE IST2430I
IST2430I 3270 DATA STREAM ERROR - NETA.TSO10002 NETA.TCPM0001 048
...
IST314I END
IEA794I SVC DUMP HAS CAPTURED: 049
DUMPID=002 REQUESTED BY JOB (USER2   )
DUMP TITLE=ISTRACSW - MSG CSDUMP - ID=6C5C
IEA911E COMPLETE DUMP ON SYS1.DUMP01 055
DUMPID=002 REQUESTED BY JOB (USER2   )
FOR ASIDS(0031,001D)
INCIDENT TOKEN: LOCAL    VIC000   02/08/2016 18:37:09
```

Example when you use the **SLIP** command.

```
SLIP SET,ENABLE,MSGID=IST2430I,ID=2430,ACTION=SVCD,JOBNAME=NET,
END
IEE725I SLIP PARAMETERS ARE- 142
ID=2430,NONPER,ENABLED
ACTION=SVCD,SET BY CONS IC000A,RBLEVEL=ERROR,MATCHLIM=1,0
JOBNAME=NET,MSGID=IST2430I
IEE727I SLIP TRAP ID=2430 SET
...
IEA045I AN SVC DUMP HAS STARTED AT TIME=14.06.53 DATE=02/08/2016 165
FOR ASID (001D)
QUIESCE = YES
IEA992I SLIP TRAP ID=2430 MATCHED.  JOBNAME=NET  , ASID=001D.
IEA411I SLIP TRAP ID=2430 DISABLED FOR MATCHLIM
IEA794I SVC DUMP HAS CAPTURED: 168
DUMPID=003 REQUESTED BY JOB (NET  )
DUMP TITLE=SLIP DUMP ID=2430
IST2424I 3270 DATA STREAM ERROR - NETA.TSO10002 NETA.TCPM0001 164
...
IST314I END
```

The VTAMMAP SES formatted dump tool will format the 3270 incidents that are found for each session. See z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures for more information.

GTF trace data

When a 3270 IDS incident occurs, trace records are written to an active generalized trace facility (GTF).

Use the following command to start GTF. To prevent prompting, add the NOPROMPT option to the GTF procedure parameter, which enables starting an automated GTF procedure.

```
S GTF.GTF,DSN=USER.TRACE,DISP=OLD,MEMBER=GTFF90
AHL121I TRACE OPTION INPUT INDICATED FROM MEMBER GTFF90 OF PDS SYS1.PARMLIB
AHL103I TRACE OPTIONS SELECTED--USR
00 AHL125A RESPECIFY TRACE OPTIONS OR REPLY U
REPLY 00,U
AHL031I GTF INITIALIZATION COMPLETE
```

Use the following command to stop GTF.

```
P GTF
AHL006I GTF ACKNOWLEDGES STOP COMMAND
AHL904I THE FOLLOWING TRACE DATASETS CONTAIN TRACE DATA :
        USER.TRACE
```

For more information about using GTF, see The Generalized Trace Facility (GTF) in z/OS MVS Diagnosis: Tools and Service Aids.

Collecting GTF trace data

Event ID (EID) records are always written to available GTF which allows the writing of the EID when a 3270 IDS incident occurs. Up to DSCOUNT outbound PIUs and the inbound PIU that caused the incident are written.

The following example shows a sample GTF procedure.

```
//GTFNEW PROC MEMBER=GTFPARM
//IEFPROC EXEC PGM=AHLGTF,'PARM=MODE=EXT,DEBUG=NO,TIME=YES',
// TIME=1440,REGION=4M
//IEFRDER DD DSNAME=SYS1.TRACE,UNIT=SYSDA,SPACE=(TRK,20),
// DISP=(NEW,KEEP)
//SYSLIB DD DSN=SYS1.PARMLIB(&MEMBER),DISP=SHR
```

The following example shows a sample GTF SYS1.PARMLIB(GTFF90) member. `F90` is the EID of the 3270 IDS trace records. `FEF`, `FF0`, and `FF1` are VTAM buffer trace EIDs.

```
TRACE=USRP
USR=(F90,FEF,FF0,FF1)
```

Formatting GTF trace data

Use the **IPCS GTFTRACE** command to format the collected generalized trace facility (GTF) data for a 3270 Intrusion Detection Services (IDS) incident.

```
GTFTRACE DSN('USER.TRACE') USR(F90)
```

For more information about the GTFTRACE command, see z/OS MVS IPCS Commands.

For each 3270 IDS incident, up to DSCOUNT outbound PIUs are traced. The inbound PIU, which contained the data stream that caused the incident to be found and recorded, is also traced. Each trace record contains information about the incident.

The following example shows the formatted 3270 IDS trace records.

```
USRFD F90 ASCB 00F8EE00           JOBN JHACKER
                                        **** 3270 Data Stream Error ****
       (1)3270    NETA.TCPM0001    /NETA.TSO0002         LRC(000,000)    OUTBOUND    COMPLETE SEGMENT
       (2)Time    UTC 2016/01/25 20:47:56.476213  LOC 2016/01/25 15:47:56.476213
       (3)Event   Token 0000000001  SID  EAABEEC3 31E8DB02  Buffer 01 of 01
       (4)IPAddr  192.168.98.254..61691
       (5)Overlap Row 009  Col 016 Offset 00665
       (6)OUT     SEQ X'0001'  Offset 00598  Length 00039
       (7)                                40404040 40404040 D1C1C3D2 E2D6D540 40404040  *        JACKSON     *
                                          40404040 00000000 00000000                    *    ........        *
       (8)IN      SEQ X'0001'  Offset 00284  Length 00039
       (9)                                40404040 40404040 F1F2F3F4 F5F6F7F8 F9404040  *        123456789   *
                                          40404040 114AE9F6 F14040D7                    *    .¢Z61  P        *
      (10)Buffer  UTC 2016/01/25 20:47:26.450328  LOC 2016/01/25 15:47:26.450328
      (11)VTAM    TH=40000000 00000000 00010001 00000001 1800000B 00580001 051F  RH=0380C0
      (12)        SEQ 0001-0001          F5C21140 402901C0 40F4F040 40E44040 40404040  *5B.  ..{ 40  U      *
                                         404040C3 C8D9C9E2 E3C9C1D5 40404040 40404008  *   CHRISTIAN       .*
...
                                         114DC829 01C0E9C5 F94040D7 40C8E240 40D44040  *.(H..{ZE9  P HS  M  *
                                         40D4C1E2 D6D54040 40404040 40404011 4DF02901  * MASON         .(0..*
                                         C06CF6C3 4040D740 4040C940 40404040 D1C1C3D2  *{%6C  P   I     JACK*
                                         E2D6D540 40404040 40404040 114ED829 01C06DF6  *SON         .+Q..{_6*
...
                                         40404040 40404040 40C8C5E7 E2E3D9C9 D5C74DF0  *         HEXSTRING(0*
                                         F05D4011 5D7E1D60                             *0) .)=.-            *
       (13)       GMT-01/25/2016 20:47:56.476251  LOC-01/25/2016 15:47:56.476251

USRFD F90 ASCB 00F8EE00           JOBN JHACKER
                                        **** 3270 Data Stream Error ****
       (1)3270    NETA.TSO0002     /NETA.TCPM0001        LRC(000,000)    INBOUND     COMPLETE SEGMENT
       (2)Time    UTC 2016/01/25 20:47:56.476213  LOC 2016/01/25 15:47:56.476213
       (3)Event   Token 0000000001  SID  EAABEEC3 31E8DB02                 CODE U('E4')
       (4)IPAddr  192.168.98.254..61691
       (5)Overlap Row 009  Col 016 Offset 00665
       (6)OUT     SEQ X'0001'  Offset 00598  Length 00039
       (7)                                40404040 40404040 D1C1C3D2 E2D6D540 40404040  *        JACKSON     *
                                          40404040 00000000 00000000                    *    ........        *
       (8)IN      SEQ X'0007'  Offset 39044  Length 00001
       (9)                                40404040 40404040 F1F2F3F4 F5F6F7F8 F9404040  *        123456789   *
                                          40404040 114AE9F6 F14040D7                    *    .¢Z61  P        *
      (10)Buffer  UTC 2016/01/25 20:47:56.476216  LOC 2016/01/25 15:47:56.476216
      (11)VTAM    TH=40000000 00000000 00000001 00010001 1C000058 000B0001 0298  RH=0393A0
      (12)        SEQ 0001-0001          7D4AD811 40E9C3F1 4040E440 40404040 D4404040  *'¢Q. ZC1  U     M   *
                                         C1D3C5E7 E8E24040 40404040 40404040 11C1F9C3  *ALEXYS           .A9C*
                                         F54040E4 4040E240 40D44040 40D4C1E2 D6D54040  *5  U  S  M   MASON  *
                                         40404040 40404040 4011C3C9 C3F94040 E440C8E2  *         .CIC9  U HS*
...
                                         40E4D540 40C940D4 404040D4 C1E2D6D5 40404040  * UN  I M   MASON    *
                                         40404040 40404011 4AC1F6F0 4040D740 40404040  *       .¢A60  P     *
                                         40404040 F1F2F3F4 F5F6F7F8 F9404040 40404040  *    123456789       *
                                         114AE9F6 F14040D7 40404040 40D44040 40D4C1C4  *.¢Z61  P     M   MAD*
                                         C9E2D6D5 40404040 40404040 40114BF9 C5F54040  *ISON         ..9E5  *
...
                                         C8C540E5 C1D3E4C5 40E3D67A 40404040 40404040  *HE VALUE TO:        *
                                         40404040 404040C8 C5E7E2E3 D9C9D5C7 4DF0F05D  *       HEXSTRING(00)*
                                         40                                            *                    *
      (13)   GMT-01/25/2016 20:47:56.476251  LOC-01/25/2016 15:47:56.476251
```

In the example:

(1) The network names of the primary logical unit (PLU) and secondary logical unit (SLU), the lost record counts, the direction of the packet (inbound or outbound), and the position of the RU in the traced records. Outbound packets trace the entire chain of RUs from the begin chain to the end chain. Inbound packets trace only the specific RU that caused the incident.

(2) The UTC and local time of the incident.

(3) A unique value for the incident, the session identifier, and code. IBM service personnel use this code to identify how the incident was discovered.

(4) If Telnet is used, the IP address and port of the secondary connection.

(5) The row and column, in the 3270 display buffer, of the field where the overlay occurred. The offset is the offset in the 3270 display buffer.

(6) The location in the outbound packet when the overlay occurred.

(7) Up to 32 bytes of the outbound packet are displayed.

(8) The location in the inbound packet that caused the overlay.

(9) Up to 32 bytes of the inbound packet are displayed.

(10) The time stamp when the buffer was captured.

(11) The VTAM transmission and request headers.

(12) The RU data. The first and last sequence numbers of the RU chain that contributed to the RU are formatted.

(13) The time stamp when the trace date is recorded.

Using SMF

The 3270 IDS incidents are written to the System Management Facility (SMF) as a series of type 119 (subtype 81) records. Each record contains a common section that describes the incident and a saved DSCOUNT outbound buffer. The last outbound SMF record for an incident contains the inbound buffer.

For more information about the record, see VTAM 3270 Intrusion Detection Services event record (subtype 81) in z/OS Communications Server: IP Programmer's Guide and Reference.

Incident validation

When an incident is reported, it must be validated by gathering documentation immediately. This documentation should include the following information:

- The time and place that the incident occurred.
- The source, which is the logical unit (LU) names of the primary and secondary LUs. If the session is a TELNET session, the source also includes the IP address of the secondary LU.
- The name and type of application that was being used; and if possible, the transaction that was being executed.
- The name of the PU, LINE, and major node of the secondary LU, if applicable.
- Additional trace data needs to be collected to determine whether a pattern of data exists to this incident.

Example

```
IST2424I 3270 DATA STREAM ERROR - NETA.TSO0002 NETA.TCPM0001
IST2425I PLU SUBAREA = X'0001' INDEX = X'0000' ELEMENT = X'0058'
IST2425I SLU SUBAREA = X'0001' INDEX = X'0001' ELEMENT = X'0009'
IST2441I JOBNAME = JHACKER SID = EAABEEC331E8DB02
IST2426I IPADDR = 192.168.98.254..61691
IST2427I DATE = 2016/01/25 TIME = 15:47:56 ID = 1
IST2428I ROW = 9 COLUMN = 16
IST2429I OUTBOUND - SEQ = X'0001' OFF = 598 LEN = 39
IST2431I 40404040 40404040 D1C1C3D2 E2D6D540  *        JACKSON *
IST2430I INBOUND - SEQ = X'0001' OFF = 284 LEN = 39
IST2431I 40404040 40404040 F1F2F3F4 F5F6F7F8  *        12345678*
IST314I END
```

- The date and time of this incident is identified in message IST2427I and in the formatted trace data. The ID shows a unique identifier for this incident and this is the first one since VTAM was started.

```
IST2427I DATE = 2016/01/25 TIME = 15:47:56 ID = 1
```

- The secondary LU is identified in message IST2424I as NETA.TCPM0001. The following information displays this LU. Message IST271I shows that this LU is an application that the job name TELNET opens. Messages IST1727I and IST1669I identify the domain service name and IP address of the user.

  Note: TCPM0001 is an application that acts as a secondary LU, which is not supported for 3270 IDS monitoring.

```
IST2424I 3270 DATA STREAM ERROR - NETA.TSO0002 NETA.TCPM0001
d net,id=NETA.TCPM0001
IST097I DISPLAY ACCEPTED
IST075I NAME = NETA.TCPM0001, TYPE = DYNAMIC APPL 456
...
IST231I APPL MAJOR NODE = TCPAPPLS
IST271I JOBNAME = TELNET, STEPNAME = TELNET, DSPNAME = IST19405
...
IST1727I DNS NAME: JOEHACKER.FARFARAWAY.EXAMPLE.COM
IST1669I IPADDR..PORT 192.168.98.254..61691
IST171I ACTIVE SESSIONS = 0000000001, SESSION REQUESTS = 0000000000
IST206I SESSIONS:
IST634I NAME     STATUS         SID          SEND RECV VR TP NETID
IST635I TSO10002 ACTIV-P     EAABEEC331E8DB02 0004 0009       NETA
IST314I END
```

- The name of the PLU application is TSO0002. This user is logged onto TSO. The following information displays the application information. Message IST271I shows the TSO user ID. Messages IST2433I and IST2434I show the application 3270 IDS parameter values. Message IST2435I confirms that an 3270 IDS data steam error occurred.

```
IST2424I 3270 DATA STREAM ERROR - NETA.TSO0002 NETA.TCPM0001
D NET,ID=TSO0002,E
IST097I DISPLAY ACCEPTED
IST075I NAME = TSO0002, TYPE = APPL 479
IST486I STATUS= ACT/S, DESIRED STATE= ACTIV
...
IST231I APPL MAJOR NODE = TSO1A
IST213I ACBNAME FOR ID = TSO10002
...
IST271I JOBNAME = JHACKER, STEPNAME = OS390R5, DSPNAME = IST71E8A
...
IST2433I DSMONITR = YES, DSCOUNT = 15, DSACTION = (CONSOLE,NONE)
IST2434I DSTRUST = LOCALLU
IST2435I SESSIONS MONITORED = 1, ERRORS DETECTED = 1
IST171I ACTIVE SESSIONS = 0000000001, SESSION REQUESTS = 0000000000
IST206I SESSIONS:
IST634I NAME     STATUS         SID          SEND RECV VR TP NETID
IST635I TCPM0001 ACTIV/E-S   EAABEEC331E8DB02 0009 0004       NETA
IST314I END

D NET,TSOUSER,ID=JHACKER
IST097I DISPLAY ACCEPTED
IST075I NAME = JHACKER, TYPE = TSO USERID 623
IST486I STATUS= ACTIV, DESIRED STATE= N/A
IST576I TSO TRACE = OFF
IST262I ACBNAME = TSO0002, STATUS = ACT/S
IST262I LUNAME = TCPM0001, STATUS = ACT/S
IST1727I DNS NAME:  JOEHACKER.FARFARAWAY.EXAMPLE.COM
IST1669I IPADDR..PORT 192.168.98.254..61691
IST2203I CHARACTER SET 02B9 - CODE PAGE 0417
IST314I END

D A,JHACKER
IEE115I 15.58.22 2016.025 ACTIVITY 638
 JOBS     M/S    TS USERS    SYSAS    INITS   ACTIVE/MAX VTAM     OAS
00000    00011    00002      00033    00003    00002/00300       00004
JHACKER OWT     A=0025   PER=NO   SMC=000  PGN=N/A  DMN=N/A  AFF=NONE
                CT=000.032S  ET=01.04.21
                WUID=TSU00029
                WKL=TSO      SCL=TSO      P=1
                RGP=N/A      SRVR=NO  QSC=NO
                ADDR SPACE ASTE=1EFD6940
```

- The information of a secondary LU might identify the PU, LINE, and major node. In this example, the information of the PU, LINE, and major node is not available. However, you can use the TCPIP commands **NSLOOKUP** and **TRACERTE** to confirm the ID and location of the secondary LU. Information about `router206` indicates the approximate location.

  For more information about TCPIP commands, see z/OS Communications Server: IP System Administrator's Commands.

```
nslookup  192.168.98.254
EZB3170I Server:  dns.example.com
EZB3172I Address:  192.168.100.4

EZB3170I Name:    joehacker.farfaraway.example.com
EZB3172I Address:  192.168.98.254
READY
tracerte 192.168.98.254
CS V2R1: Traceroute to 192.168.98.254 (192.168.98.254)
1 router65.faraway.example.com (192.168.105.65)  2 ms  0 ms  0 ms
2 router1.faraway.example.com (10.6.0.1)  1 ms  0 ms  0 ms
3 router41a.faraway.example.com (192.168.120.41)  0 ms  0 ms  0 ms
4 routeredge201.faraway.example.com (192.168.106.201)  0 ms  0 ms
5 router1a.farfaraway.example.com (192.168.184.1)  15 ms  18 ms  21 ms
6 router8.faraaway.example.com (192.168.34.8)  12 ms
7 router208.faraaway.example.com (192.168.106.208)  2 ms  9 ms  11 ms
8 router12.faraaway.example.com (192.168.96.120)  7 ms  12 ms  10 ms
9 joehacker.farfaraway.example.com (192.168.98.254)  2 ms  2 ms  1 ms
READY
```

- You can use the TCPIP **Netstat** command to show the time when the connection started.

  For more information about TCPIP commands, see z/OS Communications Server: IP System Administrator's Commands.

  Tip: Information about the IP session is recorded in type 119 SMF records. Subtypes 1 and 2 contain information about the TCP connection. Subtypes 21 and 22 contain information about the TELNET connection. For TSO sessions, type 30 records contain information about the TSO user.

```
netstat all (port 55516
 MVS TCP/IP NETSTAT CS V2R1       TCPIP Name: TCPCS           20:57:34
 Client Name: TELNET                   Client Id: 00000024
   Local Socket: ::ffff:192.168.105.112..23
   Foreign Socket: ::ffff:192.168.98.254..61691
     BytesIn:            0000000000000002422
     BytesOut:           0000000000000009580
     SegmentsIn:         0000000000000000247
     SegmentsOut:        0000000000000000320
     StartDate:          01/25/2016       StartTime:          17:33:56
     Last Touched:       20:47:56         State:              Establsh
...
     Application Data:   EZBTNSRV TCPM0001 TSO10002 ET B
 ----
 READY
```

- The following information of messages from IST2428I to IST2431I indicates the overlay in the 3270 data steam. Near row 9 and column 16 in the 3270 display buffer, a field that contains the string JACKSON is replaced by the string 12345678. Messages IST2429I and IST2430I show the respective PIUs where the fields can be found.

```
IST2428I ROW = 9 COLUMN = 16
IST2429I OUTBOUND - SEQ = X'0001' OFF = 598 LEN = 39
IST2431I 40404040 40404040 D1C1C3D2 E2D6D540  *        JACKSON *
IST2430I INBOUND - SEQ = X'0001' OFF = 284 LEN = 39
IST2431I 40404040 40404040 F1F2F3F4 F5F6F7F8  *        12345678*
```

  Tip: Message IST2431I shows part of the raw 3270 data stream, which might include different 3270 orders. The presence of the Start Field order (x'1D') might indicate that a field attribute has been overlaid, which might cause the incident report. Another order is the Start Field Extended (x'29'). For more information about the 3270 data stream, see 3270 Data Stream Programmer's Reference.

- The following generalized trace facility (GTF) trace data shows information about the buffers. Start additional traces of VTAM buffers to verify whether the sequence is repeated. The TCPIP packet trace data can also be collected. The TELNET option of the TCPIP packet trace formatter can be used to display the 3270 data stream orders.

  For more information about the TCPIP packet trace, see z/OS Communications Server: IP Diagnosis Guide.

```
      (11)VTAM    TH=40000000 00000000 00010001 00000001 1800000B 00580001 051F  RH=0380C0
      (12)        SEQ 0001-0001           F5C21140 402901C0 40F4F040 40E44040 40404040  *5B.  ..{ 40  U     *
                                          404040C3 C8D9C9E2 E3C9C1D5 40404040 40404008  *   CHRISTIAN      .*
...
                                          114DC829 01C0E9C5 F94040D7 40C8E240 40D44040  *.(H..{ZE9  P HS  M  *
                                          40D4C1E2 D6D54040 40404040 40404011 4DF02901  * MASON         .(0..*
                                          C06CF6C3 4040D740 4040C940 40404040 D1C1C3D2  *{%6C  P   I     JACK*
                                          E2D6D540 40404040 40404040 114ED829 01C06DF6  *SON         .+Q..{_6*
...
                                          40404040 40404040 40C8C5E7 E2E3D9C9 D5C74DF0  *         HEXSTRING(0*
                                          F05D4011 5D7E1D60                             *0) .)=.-            *

      (11)VTAM    TH=40000000 00000000 00000001 00010001 1C000058 000B0001 0298  RH=0393A0
      (12)        SEQ 0001-0001           7D4AD811 40E9C3F1 4040E440 40404040 D4404040  *'¢Q. ZC1  U     M   *
                                          C1D3C5E7 E8E24040 40404040 40404040 11C1F9C3  *ALEXYS          .A9C*
                                          F54040E4 4040E240 40D44040 40D4C1E2 D6D54040  *5  U  S  M   MASON  *
                                          40404040 40404040 4011C3C9 C3F94040 E440C8E2  *         .CIC9  U HS*
...
                                          40E4D540 40C940D4 404040D4 C1E2D6D5 40404040  * UN  I M   MASON    *
                                          40404040 40404011 4AC1F6F0 4040D740 40404040  *       .¢A60  P     *
                                          40404040 F1F2F3F4 F5F6F7F8 F9404040 40404040  *    123456789       *
                                          114AE9F6 F14040D7 40404040 40D44040 40D4C1C4  *.¢Z61  P     M   MAD*
                                          C9E2D6D5 40404040 40404040 40114BF9 C5F54040  *ISON         ..9E5  *
...
                                          C8C540E5 C1D3E4C5 40E3D67A 40404040 40404040  *HE VALUE TO:        *
                                          40404040 404040C8 C5E7E2E3 D9C9D5C7 4DF0F05D  *       HEXSTRING(00)*
                                          40                                            *                   *
```

DISPLAY STORUSE pools

The DISPLAY STORUSE command provides a way to remedy a possible shortage of storage space. Table 13 provides a list of storage pools that are displayed using the DISPLAY STORUSE command. Included for each pool is a short description of the pool function and characteristics. These pools are not customer-defined, unlike the buffer pools defined using the VTAM start options (for example, IOBUF). VTAM allocates and deallocates storage from these pools as needed.

If VTAM is in a storage shortage situation, Table 13 and the output from the DISPLAY STORUSE command can be used to determine where excess storage is being used, enabling you to take appropriate action to remedy the shortage.

Table 13. DISPLAY STORUSE pools

Pool name	Storage location	Description
ACDEB	SYSTEM	A pool element is allocated for every active application.
ACPCB	USER	An element is allocated for every adjacent control point with which this node has an active CP-CP session.
ADJCP	USER	Each pool element defines a single adjacent control point (ADJCP).
ADJNODE	USER	Elements are allocated for each CP-CP session partner to track topology flow status with an adjacent node.

Table 13. DISPLAY STORUSE pools (continued)

Pool name	Storage location	Description
ALPHCD	SYSTEM	Element used by HPDT MPC to manage CSM buffer descriptors. These descriptors represent the storage used for the physical transmission of data over HPDT MPC.
AMU	SYSTEM	Elements are short-lived signals used for intraproduct communication.
ANDCB	USER	One element is allocated the first time a node activates a link supporting CP-CP sessions with a specific adjacent node.
ATGB	USER	An element represents a single T2.1 connection or VR-TG to an adjacent CP.
AUTOLOGN	USER	Elements are used to keep track of autologon relationships.
BFRTRACE	SYSTEM	Elements are used to hold small buffer trace records.
BFRTRFUL	SYSTEM	Elements are used to hold large buffer trace records.
BSBEXT	USER	Elements are allocated for each session using SNA/IP support.
CAB	SYSTEM	One element is allocated for each VCNS connection resulting from a LOGON to a VCNS line (LANs) or from an X.25 OPEN command.
CACHE	USER	Elements are used for caching PCIDs during direct search list processing.
CANT	SYSTEM	One element is allocated for every 64 VCNS X.25 connections for the same LOGON to a VCNS line.
CDAJSCP	USER	Elements are used to define adjacent SSCP entries.
CDRSC	USER	Elements are used to define dynamic CDRSCs and clone CDRSCs.
CFSACCCD	SYSTEM	Coupling facility short-lived common storage pool.
CFSACCCS	SYSTEM	Coupling facility long-lived common storage pool.
CFSACCPD	USER	Coupling facility short-lived private storage pool.
CFSACCPS	USER	Coupling facility long-lived private storage pool.
CFSBUFCD	SYSTEM	Elements are short-lived buffer objects used to manage coupling facility structure data buffers.
CFSBUFCS	SYSTEM	Elements are long-lived buffer objects used to manage coupling facility structure data buffers.
CFSBUFPD	USER	Elements are short-lived buffer objects used to manage coupling facility structure.
CFSBUFPS	USER	Elements are long-lived buffer objects used to manage coupling facility structure.
CFSCSA	SYSTEM	Coupling facility common storage pool.
CFSPRIV	USER	Coupling facility private storage pool.
CMIPPVT	USER	CMIP services allocates most of its buffers from this pool.
CMOBJ	SYSTEM	Elements are used by VTAM connection manager to represent logical connections using HPDT DLCs.

Table 13. DISPLAY STORUSE pools (continued)

Pool name	Storage location	Description
CNSFACUD	SYSTEM	An element is allocated every time a VCNS application asks VTAM to initiate or receive an X.25 call request that will contain facilities or call user data.
CORCB	USER	Elements are used for APPN Locate request correlation.
COS	USER	Elements are used for APPN COS definitions and mode table mappings.
COWE	USER	One element is allocated by the VTAM topology agent for each CMIP operation request the agent processes. The element is freed when the operation ends.
CPRUPE	USER	Elements are request/response unit processing elements used when processing APPN-related requests.
CPWACSA	SYSTEM	An element is allocated when a USS command is entered from the network operator console or from a user terminal. One element from the pool is allocated when an application resource definition specifying SSCPFM=USSNOP is being processed.
CPWAPVT	USER	One element is allocated when a USS command is entered from the network operator console or from a user terminal. One element from the pool is allocated when an application resource definition specifying SSCPFM=USSNOP is being processed.
DCX	SYSTEM	Pool elements are used to maintain data compression information.
DDEL	USER	Elements are used to delay the disconnection of a PU that is defined with the DISCNT=DELAY parameter.
DECB	USER	An element is allocated for each resource in the APPN directory database.
DISKIO	USER	One element is allocated per component performing database hardening. The storage for this pool is allocated below the 16–M line.
DMTSQ	USER	One element is allocated every time a message contained in the message flooding table is issued. The allocated element is freed when the message suppression time expires.
DSERVER	USER	Elements are control blocks and short-term signals related to directory services and interchange nodes.
DSSIB	USER	An element is allocated when a DSRLST is received and freed when the DSRLIST response is sent.
DSUTIL	USER	Elements are used to perform locate search processing.
DYPATH	USER	Elements are path table entries for dynamic PUs.
EEHNMIPD	SYSTEM	An element from this pool is allocated when the SNAMGMT start option is set to YES and a client application connects to the SNA Network Management socket. More elements are allocated when a response is built because of a request from a client application. These additional elements are freed when the response is returned. The original element is freed when either the client or VTAM terminates the connection.
EPTDVT	SYSTEM	Elements are used to contain DLC-specific information.

Table 13. DISPLAY STORUSE pools (continued)

Pool name	Storage location	Description
ERICPOOL	USER	Elements are used while parsing request/response units. When the RU processing completes, the elements are freed.
ERTE	USER	Elements are used to define explicit routes resulting from PATH statements.
FMCB	SYSTEM	Elements are allocated once for each session associated with an application LU (for nonpersistent LU sessions) at session BIND time.
FMCBEXT	SYSTEM	Elements are allocated once for each session associated with an application LU at session BIND time.
FMH5	SYSTEM	One element is allocated for each incoming LU 6.2 conversation request.
GRINS	USER	Elements are used to maintain associations between network resources and generic names.
GWNAJSCP	USER	Elements are: • Adjacent SSCP routing tables used to route CDINIT or DSRLST RUs. Elements are freed when the routing completes or fails. • Information to determine the gateway NCP to use during session setup.
HIPOOLPS	USER	HPR table used by MNPS
HPRINFO	USER	Elements exist for each RTP connection for which data is being collected by a single performance monitor application.
HSICB	SYSTEM	Elements are allocated once for each APPC session associated with an application LU at session BIND time.
HSQH	SYSTEM	Elements are allocated once for the first of every 107 sessions set up across a VR, at session BIND time.
IOBLOCKL	SYSTEM	Elements in the pool are large DLC-related control blocks (for example a channel-attached NCP). The storage for this pool is fixed and is not paged out of memory by the operating system.
IOBLOCKP	USER	Elements in the pool are large DLC-related control blocks. The storage for this pool is not fixed and can be paged out of memory by the operating system.
IOBLOCKS	SYSTEM	Elements in the pool are small DLC-related control blocks (such as for a channel-attached NCP). The storage for this pool is fixed and is not paged out of memory by the operating system.
IOSIB	USER	Elements are used to process Init_Other (Cross-domain) requests.
IPADDR	USER	Element used to store IP addresses and host names.
ISTENDEL	USER	One element is allocated by a network node for each adjacent served end node or nonnative network node.
ISTSITCB	USER	One element is needed at endpoint and network node server roles for each APPN Search procedure.
ISTTRCEL	USER	Elements are used for the problem determination (PD) trace function of the CNM interface.

Table 13. DISPLAY STORUSE pools (continued)

Pool name	Storage location	Description
KEYTOKEN	SYSTEM	Elements map active cryptographic session key tokens.
LCB	USER	An element is allocated to process locate search requests.
LMTABLE	SYSTEM	Three types of elements come from this pool: • One element is allocated for every pair of LUs that have negotiated APPC session limits. The element is allocated when a CNOS with a partner LU is initiated, and freed when the application closes its ACB. • An element is used for every application that opens its ACB with APPC=YES. • Elements represents current session limits between two LU 6.2s on a particular mode. An element is allocated for every logmode that has been negotiated between two partner LUs. The elements are freed for deletion, or freed when the application closes its ACB.
MARB	USER	Elements are allocated by the VTAM topology agent when the agent sends response data to CMIP services. Elements are freed when the agent is notified that data was received.
MRPOOLPS	USER	Elements contain MNPS RTP information.
NDREC	USER	Elements are used for APPN topology node information.
NIDCB	USER	An element is allocated for each network identifier known to the APPN directory database.
NLPDELPD	USER	Elements contain MNPS NLP entry IDs.
NQDAT	USER	One element is allocated for each network-qualified SRTE.
NSRUL	SYSTEM	Elements are used to process LU 6.2 session activation. NSRUL is used for larger-sized requests.
NSRUS	SYSTEM	Elements are used to process LU 6.2 session activation. NSRUS is used for smaller-sized requests.
NSS	SYSTEM	Elements are used to process LU 6.2 session activation.
OSCB	USER	Elements are used to track outstanding locate search requests.
PAGBLBSB	USER	Elements are allocated for each session using HPR or SNA/IP support.
PAQ	USER	Elements are used to track PLU network addresses for a given LU.
PCDCA	USER	Elements are used for border node PCID caching.
PGIOBLK	SYSTEM	Elements are used when communicating with the 3172 or the OSA.
PLOCB	USER	Elements are used to process locate search requests and replies.
PLUSC	SYSTEM	Elements are used during persistent LU session CLOSE processing.
PLUSDATA	SYSTEM	Elements are allocated once for each persistent LU session associated with an application LU, at session BIND time. An additional element is allocated for each MNPS session at session BIND time.

Table 13. DISPLAY STORUSE pools (continued)

Pool name	Storage location	Description
PLUSFMCB	SYSTEM	Elements are allocated once for each persistent LU session associated with an application LU, at session BIND time.
POAPRIV	USER	One element is allocated for each message destined for a program operator application (POA). If the message requires a reply, a second POAPRIV element is allocated.
POWECOMM	SYSTEM	One element is allocated for every message issued when VTAM is running under a user task.
POWEPRIV	USER	One element is allocated for every message issued when VTAM is running under the VTAM task.
POWMCOMM	SYSTEM	One element is allocated for every single-line message and for every message group when VTAM is running under a user task.
POWMPRIV	USER	One element is allocated for every single-line message and for every message group when VTAM is running under the VTAM task.
PRDLE	SYSTEM	Elements represent random data being used for establishing LU 6.2 sessions with session-level security.
PRIDBLK	USER	Elements map procedure-relation identifier blocks (PRIDs)
PRIDQAB	USER	Elements are used to maintain procedure-relation identifier blocks (PRIDs).
PULURDTE	USER	Elements are used to define dynamic and predefined PUs and LUs.
PVTSTATC	USER	Generic utility pool for large blocks of storage that must be in VTAM private storage for an extended period of time.
PXBFIXED	SYSTEM	Elements are used to expand fixed buffer pools. The storage for this pool is fixed and is not paged out of memory by the operating system.
PXBPAGED	SYSTEM	Elements are used to expand pageable buffer pools.
RAB	SYSTEM	One element is allocated for each APPC conversation.
RAQ	USER	Elements are used to queue requests when a usable network address is not available and an RNAA must be sent.
RIBRANT	SYSTEM	One element is allocated for each LOGON of a VCNS application to a VCNS line, plus one extra element for every 16 LOGONs.
RPMNPSPS	USER	RTP elements used by MNPS
RTPINFO	USER	Contains a number of different elements, all of which are used for HPR. Both the RTP and RCM components use this pool.
RUCON	USER	One element is allocated each time a DISPLAY ROUTE,TEST=YES command is issued. After 168 elements have been allocated, VTAM will delete any elements that have not been used for more than 30 minutes.
RUPECOMM	SYSTEM	Elements are allocated from this pool to process request/response units (RUs) when execution is taking place in the VTAM address space.

Table 13. DISPLAY STORUSE pools (continued)

Pool name	Storage location	Description
RUPEPRIV	USER	Elements are allocated from this pool to process request/response units (RUs) when execution is taking place in a non-VTAM address space.
SAB	SYSTEM	One element is allocated for each APPC session.
SCCB	USER	Elements are used to perform search concentration.
SIB	USER	One element is allocated for each LU-LU session.
SIBEXT	USER	One or two elements are allocated for each cross-network session. The elements are freed when the session ends.
SIBIX	USER	One element is allocated during session initiation. The element is freed when the session becomes active.
SLD	SYSTEM	Elements are allocated to process APPCCMD CONTROL=OPRCNTL,QUALIFY=DISPLAY macro instructions, including those issued from the operator console.
SLENT	USER	A pool element is allocated when a CPSVCMG session is activated between an end node and serving network node, or for any CP SNASVCMG sessions that VTAM management services transport activates.
SM3270	HVComm	Primarily used to contain 3270 screen maps. CSM HVCOMM is used for this pool.
SPTPOOL	SYSTEM	Holds all of the SPTAEs for the associated pools.
SRTE	USER	Elements are entries in the symbol resolution table.
SSCPFMCB	USER	One element is allocated for each SSCP-PU or SSCP-LU session.
STB	USER	Elements store information concerning a T2.1 adjacent link station that an independent LU is using for session connectivity.
TCPIOCD	SYSTEM	TCP/IP IO buffer pool used for QDIO.
TGP	USER	One element is created for each TG profile (TGP) entry.
TGREC	USER	Elements are used for APPN topology TG information.
TIPACX	SYSTEM	Elements contain control information to support HPDT services. The storage for this pool is fixed and is not paged out of memory by the operating system.
TREEBLD	USER	Elements are used for APPN routing tree construction and maintenance.
TRSINFO	USER	Elements are used for topology broadcast lists (for use during topology database update broadcasting) and endpoint TG vector information (during route calculation).
UECB	SYSTEM	One element is allocated each time a user exit is to be scheduled.
UNSOL	USER	An element is allocated for every adjacent control point with which this node has an active CP-CP session.
UTILCSAL	SYSTEM	Generic utility pool for large blocks of storage that must be in CSA.
UTILCSAS	SYSTEM	Generic utility pool for small blocks of storage that must be in CSA.

Table 13. DISPLAY STORUSE pools (continued)

Pool name	Storage location	Description
UTILPVTL	USER	Generic utility pool for large blocks of storage that must be in private storage.
UTILPVTS	USER	Generic utility pool for small blocks of storage that must be in private storage.
UVRPL	USER	One element is allocated each time a user exit is to be scheduled.
VRDCB	SYSTEM	An element exists for each virtual route for which data is being collected by at least one performance monitor application.
VRPL	SYSTEM	Elements are VTAM copy of an application request parameter list (RPL). Elements are also used for BINDs and other RUs received from the network.
VRRSB	USER	An element exists for each virtual route for which data is being collected by a single performance monitor application.
WAR	USER	Elements represent autologon session originators (OLU-SLU) waiting for the availability of a required PU resource.
WREEID	USER	Elements are used to suspend and resume VTAM processes.
XNINFO	USER	Elements are used for search processing.

Note: Unless otherwise specified:

- All pool storage is pageable and can be paged out of memory by the operating system.
- All pool storage can be located above or below the 16M line.
- Some of the pools above are defined to be associated with certain VTAM tasks. Pools are associated with VTAM tasks to improve performance during storage allocation. The DISPLAY STORUSE command will not display usage for the associated pools. The total storage used does account for storage allocated by these pools

Index

Numerics

A

C

D

E

G

H

I

L

M

N

P

S

T

V

Printed in USA